INFORMATION TECHNOLOGY ADMIN

POLICIES & PROCEDURES

Manual

KG REDDY College of Engineering & Technology
UGC AUTONOMOUS
NAAC ACCREDITED A+ GRADE
NBA NATIONAL BOARD OF ACCREDITATION (CSE & ECE)

Approved by AICTE, Affiliated to JNTUH.

TABLE OF CONTENTS

1. INFORMATION TECHNOLOGY ADMIN POLICIESAND STRATEGIES

POLICY FRAMEWORK

This section of the policies of the KG Reddy College of Engineering & Technology covers the management of the technology. The establishment of these policies is the responsibility of the Board of Directors. The development of these policies is a continuous process, and will require revisions of current policies, or the development of new policies to handle new situations and issues as they arise.

The KGRCET IT Admin develop these policies in accordance with governmental regulations, and periodically appraise the effects of its policies and makes revisions as necessary. KGRCET operates according to these policies established by the Board of Directors. The Board of Directors further entrusts the KGRCET IT Admin to implement them through more specific regulations and procedures. The responsibility to follow these policies is placed on all of the staff employed by KGRCET.

STRATEGIC PLANNING

The Information Technology Admin Department shall conduct periodic assessment of services to determine areas of need and provide a planned approach and determination of goals to satisfy those institutional needs.

PURPOSE

A) Insure the strategy follows the current vision and mission of the institution.
B) Focus on the major challenges for the next five years.
C) Apply resources to implement the plan and strategies for optimizing them.
D) Allocate responsibilities across KGRCET to achieve the plan.
E) Guide KGRCET in its planning and examine available / projected budget to ensure that proposed activities will fall within funding restrictions.

2. INFORMATION TECHNOLOGY ADMIN SUPPORT

HELP-DESK

All Requests for support will be logged, given a priority, and assigned repair time. Response to help desk calls will be…

- Within one working days on the highest priority
- Two days on normal priority and
- Four days on the lowest priority.

This response period does not mean the problems will be solved within this time but that the technician will look at the problem and establish the corrective action. If additional time is required (i.e. ordering of parts), the user will be notified, and a spare piece of equipment will be given if available.

TIMES OF OPERATION

Monday through Saturday 9am – 4pm (Lunch 1:10PM to 1:40PM). Support can be provided during evenings and weekends with advance notice and with approval of the Director of Information Technology.

TYPES OF REQUEST/CONTACTING INFORMATIONTECHNOLOGY ADMIN

In an effort to provide the best services by the Information Technology Admins various options listed below to secure support for technology issues. The Information Technology Office also prioritizes work orders to insure more critical issues receive quicker attention.

E-MAIL SUBMITTED WORK ORDER

At this point in time the preferred method of submitting a request for support is through e-mail. Requests should be sent to the Information Technology Department E-mail List. The subject line should have the word Work Order typed. In the body of the E-mail include the nature of the problem.

WALK-IN

Requests for support may be submitted in-person to the Helpdesk staff.

PHONE

- Information Technology Admins are available for questions regarding application issues or other issues, where the users can be guided through the problem.
- If possible Information Technology Admins may utilize software that allows for viewing of the user's desktop or may require the user to log off of his/her workstation.

- If the Help Desk technician is unable to correct the problem through phone support, the call will be logged, given a priority, and assigned repair time.

INFORMATION TECHNOLOGY ADMIN OFFICE CONTACTS		
Help-Desk	K.Chidambara Chari Mob: +91-9618929181	Log-in problems, e-mail issues, application support, computer maintenance and repair, IVN Meeting and room issues, media cart requests, printing.
Network Engineer	Y. Venkata Rao Mob: +91-9441911191	Network (WAN/LAN/wireless issues, Classroom software systems, & Print Service Issues.
Director of Information Technology	M. Saidi Reddy Mob: +91-9963850858	KGRCET Web Site corrections, KGRCET Facebook Administration, Marquee, purchasing, Scheduling , Server Issues, Other

WEB

At this time KGRCET doesn't have a web based Help Desk Portal.

INTERCOM

Requesting support through this manner does not guarantee a quick response, as many areas of KGRCET do not have phone/intercom service. Users should only utilize this method for *high priority requests* and be supplemented with an e-mail request.

EMERGENCY/ WEEKENDS

Emergency support is available after hours and weekends with approval of the Director of Information Technology.

WORK ORDER PRIORITY

- Each call will be logged based on the following ranking criteria. In the event of a high priority call arrives and conflicts with a low/normal call, the high priority call shall be given first response, even if work has begun on the low priority call.
- In some instances it may not be possible to resolve a particular problem or return to the way it worked before the problem. If the problem restricts operational performance, a different approach or alternative solution may be recommended. (i.e. send out for third party repair, return to vender or manufacturer).
- The Director of Information Technology will set priorities when there are several problems of the same priority based on when the calls were received. The Director will have final authority on what priority calls will have and the order they are

processed if questions arise.

HIGH OR EMERGENCY

- Campus-wide issues such as.
- No campus internet, E-mail, Access to web sites.
- The user(s) cannot work due to computer/network problems.
- The workstation(s) or a key program(s) is completely unusable and the workstation is required to do normal work.

Or

A class that is planning on using technology where no other equipment can be used. (ie. computer/video projector)

Or

A problem was previously logged and has not been resolved after a reasonable amount of time (generally three days)

NORMAL

- The computer is functioning but an application/file/peripheral is not functioning.
- The problem is significant but not severe enough to prevent fulfillment of normal duties or duties that cannot be carried out through other means. Examples could include a corrupted Office file, email errors, an error message that can be bypassed, a computer move/install, slow network/application service, a broken CD drive. All A/V repairs will be assigned a normal priority.

LOW

The computer is functioning normally except a minor irritant.
Example: A broken Windows key on the keyboard, screen is faded, missing icon, voice mail, inter-office computer moves.

NON-KGRCET COMPUTERS

Service to non-KGRCET computers is provided only on a time available basis.

- The client acknowledges that he/she has backed up any and all data before relinquishing the computer to the Help-Desk staff.
- The client assumes all risk of loss from any and all causes or in any way related to or resulting fromthe repair or service by KGRCET Help-Desk staff.
- The client must provide any relevant and official recovery or operating system discs for reinstallation. This also includes anythird-partysoftware such as anti-virus.

- The client shall be responsible for any parts or software needed.

UNSUPPORTED SERVICES & EQUIPMENT

The Help-Desk will provide "best effort" assistance for unsupported applications and products.

- If the Help Desk is unfamiliar with an unsupported application or product, assistance will be provided if possible. In cases where extensive research needs to be taken before assistance can take place, no support may be provided or require the approval of the Director of Information Technology.
- Hardware and software purchased without Director of Information Technology approval be will categorized as '*Unsupported*'.

NEW STAFF & FACULTY

ORIENTATION

All new staff & Faculty will be given a short introduction into the various systems such as;

- Using their Network username and password to log into their workstation.
- Microsoft Outlook and Web Mail.
- Printing.
- Accessing the College Web Sites.
- For Faculty: Logging onto CMS (College Management System) and Ion Cudos.

COMPUTER AND SOFTWARENEEDS

KGRCET Departments / Programs hiring staff into newly created positions are responsible for purchasing new workstations and software. Departments requiring additional software should explore available grant funding before purchasing through general fund budgets. The Information Technology Admin Department can (if available) set-up a temporary workstation upon request from the department administrator.

COLLEGE MANAGEMENT SOFTWARE(CMS) AND ACCOUNTS

Only positions requiring CMS software shall have access to this software. Staff that requires this software for their position shall receive:

- CMS Account.
- Given membership in the Active Directory Security Group: kgr.ac.in.

LAPTOP / COMPUTERCHECK-OUT

All Laptops / Computer purchased by the KG Reddy Engineering College & Technology will be checked –out through the KGRCET Information Technology Admin Department to insure proper tracking and maintenance of college laptop / computers.

STAFF LEAVING EMPLOYMENT

NETWORK ACCOUNTS

- Mailing List (Distribution/Security) memberships are removed upon termination of Employment.
- E-Mail accounts are disabled for a period of 30 days and then deleted. If Supervisors need to view e-mail of the past employee, they will have the 30 day period to do so.
- Computer documents from their documents folder, desktop, and Internet links that are pertinent to the staff or faculty members' position will be backed up to a network folder to await transfer to new personnel or review by the supervisor.
- Documents that need to be shared through the Department should be relocated to the Departments site.

OTHER ACCOUNTS &PASSWORD

- Out-going staff and faculty are required to relinquish any work related external account information to their supervisor that would make for a smooth transition to the new employee. This should include links, and passwords.
- If possible the supervisor should take ownership or update Point ofContact information before the employee completes their Exit Interview.
- It is highly recommended that Supervisors take ownership of external

accounts by changing the Point Of Contact in the interim.

TECHNICAL ASSISTANCE

TRAINING

The Information Technology Admin Department staff is available for faculty or student training dependent on available time and schedule of the Information Technology Admin staff. Any requests for Training should be submitted to the Director of Information Technology.

PURCHASING AND PLANNING

The Director of Information Technology shall evaluate technology purchases to ensure up-grade ability, compatibility, and integration with current and future programs (hardware, software, and networking).

3. NETWORK ACCOUNTUSAGE

AUTHORIZED USE

- KGRCET provides Network access only to authorized users for the purposes directly related to your employment or study at KGRCET.
- Use for any other purposes may lead to suspension or withdrawal of access, or in the more serious case to action under KGRCET disciplinary procedures.
- Please keep your passwords secret. If your password has been compromised, change the password or notify the Information Technology Admin Office immediately.

LOCAL AREA NETWORK ADMINISTRATOR ROLES

DOMAIN ADMINISTRATORS

- A person who is a member of the Domain Administrator group can create, delete, and manage all objects that reside within the network domain in which they are administrators.
- They can also assign and reset passwords and delegate administrative authority for network resources to other trusted users. Only members of the Information Technology Department may be members of this group.

LOCAL ADMINISTRATORS

- On Windows-based computers, a user account that is a member of the computers' local Administrators group or a member of a group that is a member of the local Administrators group, such as the Domain Administrator group in a Windows domain.
- This is the first account that is created when you install an operating system on a new workstation, stand-alone server, or member server. By default, this account has the highest level of administrative access to the local computer.
- In special instances Staff and faculty may be granted membership in this group. Requests for addition to the Local Administrator Group must be made to the Director of Information Technology.
- Membership to this Group can be revoked if the privilege is abused KGRCET Policy.

USERNAME CONVENTION

The standard KGRCET username convention for staff and faculty to access KGRCET network resources comprises the first initial of the first name, followed by the letters of their last name. If a username is already in use, the first two letters of the first name will be used and the letters of their last name. If the username should be cause for ridicule or communicate some other meaning, an alternate username is acceptable.

PASSWORDS

Passwords will not be re-set over the phone. Supervisors can request subordinate staff members password reset to allow temporary access. Passwords cannot be blank or the word "password" and should follow the rules for creating a strong password: An ideal password is long and has letters, punctuation, symbols, and numbers.

- Whenever possible, use at least 14 characters or more.
- The greater the variety of characters in your password, the better.
- Use the entire keyboard, not just the letters and characters you use or see most often.

E-MAIL

All full-time staff and faculty are provided with a KGRCET E-mail account. Staff and faculty utilize Gmail e-mail source, which can be accessed through the internet.

KGRCET E-mail is the official means of contact for KGRCET staff & Faculty. All official KGRCET E-mail correspondence will be delivered to these addresses.

PURPOSE OF THEPOLICY

In order to satisfy the need for timely and efficient communication, and to provide a better service to its staff and faculty, KGRCET has instituted a policy that establishes E-mail as an official means of communicating with their staff and faculty. This is motivated by the convenience, speed, cost-effectiveness, and environmental advantages of using e-mail rather than printed communication.

SCOPE

This e-mail policy provides guidelines regarding the following aspects of e-mail as an official means of communication:

- Use of E-mail;
- Assignment of E-mail addresses;
- Redirection of E-mail;
- Educational uses of E-mail;
- Appropriate use of E-mail;

- Account Limitations and Data Backup;
- Account Expiration/Termination;

USE OF E-MAIL

The use of the KGRCET E-mail system is a privilege, not a right. Users are expected to honor this policy and comply with the rules of usage and etiquette. Users are expected to check their email on a frequent and consistent basis in order to stay with current with KGRCET-related communications.

ASSIGNMENT OF E-MAILADDRESSES.

All staff and faculty will be provided with an official KGRCET E-mail account as part of the Registration process. It is to this official address that KGRCET will send E-mail communications.

REDIRECTION OF E-MAIL

In special circumstances any Staff/ Faculty may have E-mail electronically redirected to another e-mail address. If the user wishes to have E-mail redirected from his or her official KGRCET account to another E-mail account (e.g., @gmail.com, @hotmail.com), they may do so, but at his or her own risk. The KGRCET account remains as their official E- mail address and a copy is forwarded to their Second account.

1. KGRCET willnot be responsible for the handling of e-mail byoutside e-mail servers.
2. The users must make the request in person and show proof of identity and additional e-mail account access.
3. Email lost as a result of redirection *does not* absolve the user from responsibilities associated with communication sent to his/her official KGRCETemail address.

EDUCATIONAL USES OF E-MAIL

Faculty determines how E-mail will be used in their classes, but it is highly recommended that faculty include their E-mail requirements and expectations in their course syllabi.

APPROPRIATE USE OF E-MAIL

Use of the KGRCET E-mail system allows the users to conduct collaborative work efforts and share information with students, professors, and other individuals regardless of time and/or geographic boundaries.

Because of this open freedom, and the possibility of conversing with individuals with whom you may have never met, users should conduct themselves in an appropriate manner during their communications.

Every e-mail message sent from your KGRCET account carries KGRCET's name, and all communications should reflect that.

- Ingeneral, E-mail is not appropriate for transmitting sensitive or confidential information unless its use for such purposes is matched by an appropriate level of security.
- Design Guidelines:

1. Keep bulk mail short and withoutattachments.
2. Always use a clear, specific and non-empty subject line.
3. Do not attach personal, confidential, or sensitive information.

- Confidentiality regarding student records should be protected. All use of E-mail, including use for sensitive or confidential information should be consistent and protected.
- E-mail shall not be the sole method for notification of any legal action.
- KGRCET maintains the right to access user email accounts in the pursuit of an appropriately authorized investigation, but will not normally be monitored by staff unless there is a suspicion of improper use.

INAPPROPRIATE USE

- It is unacceptable to send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person.
- Use of electronic mail systems for any purpose restricted or prohibited by copyright laws or regulations.
- Attempting unauthorized access to electronic mail or attempting to breach any security measures on any electronic mail system, or attempting to intercept any electronic mail transmissions without proper authorization.
- The college e-mail service is not provided for private or personal use. Incidental personal uses of the e-mail system are permitted as long as they do not violate the law, restrictions that derive from the college's tax-exempt status, or KGRCET Policies.
- The KGRCET e-mail services may not be used for commercial or profit-making purposes unrelated to College business.

E-MAILACCOUNT LIMITATIONS(QUOTAS) ANDBACKUP Due to finite resources, KGRCET reserves the right to restrict the amount of user storage space on the email server as necessary. The KGRCET E-mail system is a communication system and is not a storage or archival system. Messages in the system are of a temporary nature and KGRCET

does not perform any archival of these messages. It is the user responsibility to archive any messages that he/she wishes to permanently maintain by printing, exporting or archiving to a portable storage.

AIL QUOTAS

- To provide a fair E-mail service to all users, there is a quota applied to the amount of E-mail each user can store on the server.
- Users will receive a warning when they are approaching their quota usage, and will see a message indicating how much E-mail they have stored when using the Web-based e-mail system.
- When the user exceeds their storage quota they will no longer be able to receive any new e-mail.
- To prevent this from happening users are encouraged to delete e-mail messages they no longer need, and to download old messages to their local computer and delete them from the server.
- These limits are:
    - For Board of Directors: 500 megabytes.
    - For Staff & Faculty: 250 megabytes.

ACCOUNT EXPIRATION/TERMINATION

Network accounts and email are deleted on a periodic basis to conserve storage space on KGRCET e-mail servers. All e-mail accounts of staff & faculty that leave employment at KGRCET are disabled upon completion of their Exit Interview and removed from any security group memberships for a thirty-day period before deletion. It is the responsibility of the staff or faculty supervisor to notify the Information Technology Admin Department of an employees' departure from employment.

DISCLAIMER

- KGRCET assumes no liability for direct and/or indirect damages arising from the user's utilization of the KGRCET e-mail system and services.
- Users are solely responsible for the content they disseminate.
- KGRCET is not responsible for any third-party claim, demand, or damage arising out of use of the KGRCET e-mail systems or services.
- By accessing and using the KGRCET staff/faculty e-mail system, you agree to abide by the above policies of KGRCET.

4. NETWORKS ANDCOMMUNICATIONS

NEW INSTALLATIONS

The installation of network cabling for new or redeveloped buildings and rooms is the responsibility of the Project Coordinator for development. Funding for all new network infrastructure, for example, connectors, routers and cables should be billed into the project. The Director of Information Technology shall be consulted on all new network installations. Upon completion all new copper and fiber connections the work shall be performance verified.

WIRING STANDARDS

The Information Technology Admin Department sets minimum cabling standards for all network installation at KGRCET. All new installations, upgrades or redevelopments must conform to these standards.

CAT-6 COPPERCABLING

The Category 6 portion of the cabling system shall comply with the proposed link and channel performance requirements of the latest revision of TIA/EIA 568-B.2-1 “Performance Specifications for 4-pair 100 Ohm Category 6 Cabling”, NEC, NRTL listing, and manufacturer's recommendations and instructions. Cable length will not to exceed 295 feet.

General Cable, Superior Essex, or Belden meeting the following characteristics at 250 MHz.

- ACR: 14.4 dB min. @100m
- PSACR: 12.4 dB min. @100m
- PSNEXT 43.3 dB min.
- ACRF 23.8 dB min.
- NEXT: 45 dB min.
- PSACRF 23.8 dB min.
- INSERTION LOSS 30.9 max.
- LCL 26 dB min.
- Return Loss 19 dBmin.
- ELTCTL 5 dB min.

FIBER-OPTIC CABLING

All Fiber-optic cabling shall be 6 strand multi-mode fibers from MDF to all IDF locations. Only .50/125um multi-mode fiber with LC or SC ends shall be utilized. All fiber to meet OM3 10Gig specs.

WORK AREA COMMUNICATIONOUTLETS

Each department must have at least one communications outlet. Each communications outlet should be sized to accommodate one Category 6 cables and connectors.

Communications outlets should be within 3 feet of an electrical outlet and installed at the same height, unless otherwise specified.

Communications outlets should be placed so that the work area or workstation cable does not exceed 5 meters (16 ft) in length.

This length is figured into the total horizontal cabling length and must not be exceeded.

CABLING SYSTEM LABELING

At a minimum, the labeling system shall clearly identify the following components of the system: racks, patch panels and outlets.

Racks and patch panels shall be labeled to identify the location within the cabling system infrastructure.

All labeling information shall be recorded on the as-built drawings and all test documents shall reflect the appropriate labeling scheme.

CABLING PATHWAYS

Pathways will be constructed from J-hooks or other suitable communications cable trays or raceway. Open cable tray is the preferred method of installation. Cable pathways shall be so designed to avoid EMF and RFI interference.

Common causes of this interference are fluorescent lighting fixtures, air handling motors and many kinds of electrical control including starters, lighting contactors, and power distribution panels. Never run parallel with electrical conduits or strap to them. Every cable, whether an individual or many grouped together, shall be supported.

Wherever possible, cable shall be grouped together in pathways. Plastic cable ties should not be used; they deform the outer cable jacket causing cable performance problems in the future (use of Velcro straps is recommended for cable management. Route open air cables (where not in raceway or cable tray) parallel or perpendicular to building construction supporting with specified products, maximum 4'-0” on center. Bending radius shall be minimum 1 inch. All cable runs shall be continuous, with no splicing.

NETWORK MANAGEMENT

Network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems.

- The Information Technology Admin Department reserves the rights to disconnect any network port whose activity causes an adverse effect on the network or on any other user. Network connections may also be revoked in the case of malicious or inappropriate computing activity on the network.
- The Information Technology Admin Department reserves the right to restrict access to the network during expansion, or for diagnostic and maintenance services. Every effort will be made to provide advance notification and schedule such disruptions during times of minimum impact and traffic.

NETWORK SECURITY

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator.

FIREWALLS

The purpose of this document is to establish an understanding of the function that a firewall plays in the overall security of KGRCET's network. All connections to the KGRCET network must pass through a network firewall. Network firewall configuration rules and permissible services rules must not be changed unless permission is obtained from the Director of Information Technology.

Given the nature of KGRCET's academic environment, the campus firewall cannot be configured to typical industry accepted standards. KGRCET does not constrict all unnecessary traffic; it is open to all traffic and denies access as needed. Due to individual security needs, depending on the type of information to be protected, the following information should be used to maximize the security of the network environment.

The Network Time Protocol (NTP) or another appropriate mechanism is used to synchronize the logs with other logging systems such as intrusion detection. In addition to examining logs, the Executive Director of

Communications and Networking periodically reviews the configuration of the firewall to confirm that any changes made are legitimate.

ROUTING AND SUBNETTING

RESERVED IP ADDRESSRANGES

Some infrastructure situations have to use static addressing, such as when finding the Domain Name System (DNS) host that will translate domain names to IP addresses. Static addresses are also convenient, but not absolutely necessary, to locate servers inside an enterprise. An address obtained from a DNS server comes with a time to live, or caching time, after which it should be looked up to confirm that it has not changed. Even static IP addresses do change as a result of network administration

- Servers
- Printers
- Wireless Access Points

NETWORK REMOTEACCESS

Remote access is a privilege granted to certain individuals who have a demonstrated need to perform mission-specific activities using enterprise resources while situated off campus. It may not be possible for everyone to receive the privilege of remote access.

These standards are designed to minimize the potential exposure to KGRCET from damages which may result from unauthorized use of KGRCET resources.

Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical internal systems, etc. A person's request for remote access to information systems that contain sensitive data must be documented in writing and authorized by his or her supervisor.

- ✓ Remote access must be strictly controlled through the same on-campus authentication and authorization measures. Logon information may not be shared with others. Unauthorized people (including family and friends) are not allowed to use KGRCET resources.
- ✓ Workstations owned by staff & faculty members, contractors or other affiliates of KGRCET must have anti-virus/anti-spyware software installed with the latest virus definitions.
- ✓ Data transmitted between remotely situated workstations and the network must be encrypted (128-bit minimum length). Acceptable mechanisms of encryption include either institutionally approved VPN or browser-based

SSL connections.

- ✓ Points for remote access entry into KGRCET networks must be configured to drop inactive connections after 30 minutes whenever possible. Using contrivances to circumvent this requirement is prohibited.

WIRELESS ACCESS

The purpose of this policy is to define standards, procedures, and restrictions for connecting KGRCET internal network(s) or related technology resources via any means involving wireless technology.

- o Wireless networks should not be considered a replacement for a wired network. They should be seen solely as extensions to the existing wired network, and are to be used for general purpose access in areas of transient use, such as common areas or meeting rooms. Wireless segments should not be used for work sessions involving any form of access to sensitive organizational data.
- o Addition of new wireless access points within KGRCET facilities will be managed at the sole discretion of the Information Technology Department. Non-sanctioned installations of wireless equipment, or use of unauthorized equipment within the organizational campus, are strictly forbidden. This policy is complementary to any previously-implemented policies dealing specifically with network access and remote access to the enterprise network.

- o The Information Technology Admin Department reserves the right to turn off without notice any access port to the network that puts KGRCET systems, data, users, and clients at risk.
- o The wireless access user also agrees to and accepts that his or her access and/or connection to KGRCET networks may be monitored to record dates, times, duration of access, data types and volumes, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.
- o Failure to comply with the above Wireless Access Policies may result in the suspension of remote access privileges, disciplinary action, and possibly termination of employment.

5. APPROPRIATE USE AND INFORMATION SECURITY / CONFIDENTIALITY

PURPOSE

To provide KGRCET faculty, staff, and students with accessible and professional computing facilities and establish appropriate terms, conditions, and restrictions on the use of said facilities. This appropriate use policy covers all computing assets of KGRCET. "Computing assets" includes but is not limited to all networks, desktop computers, servers, printers, e-mail services, web services, and any computer access. By using any KGRCET computing asset, the user agrees to all the following policies outlined in the policy.

POLICY

INFORMATION USE

- Followstandardsecuritypracticessuchasmaintainingpasswordsecrecyandloggingout of accounts when not in use;
- Use it only as required in the performance of theirjobs;
- Use it only as required in the performance of theirjobs;
- Disclose confidential information to other staff on a need-to-know basis; and
- Exercise due and diligent care to protect data and information from unauthorized access, use, disclosure, alteration, or destruction.

KGRCET DATABASE ACCESS

Under no circumstances shall student, alumni, or employee data designated as confidential be extracted and/or stored on computer systems external to KGRCET enterprise databases maintained by the Director of Information Technology without express written permission from the KGRCET Director of Information Technology.

Confidential data elements covered by this policy include:

- Adhar Card Numbers
- Birthdates
- Driver's License Numbers
- Credit Card Numbers
- Bank Account Numbers
- Routing Information

PRINTING REPORTS FROM KGRCET DATABASE SYSTEMS

Printed reports containing one or more of the data elements listed above may only by created and printed by the office responsible for the data.
The reports shall be used in a "need to know" manner and shall be kept in a confidential environment.
Paper reports containing Adhar Card Numbers or other confidential information may not be thrown in the trash, but should be shredded or returned to the originating office for proper disposal.

DEPARTMENTAL DATABASES AND REPORTS

Faculty or staff maintaining databases and/or copies or printed reports containing Adhar Card Numbers or other confidential information is personally responsible.

BACKUP POLICY

PURPOSE

The purpose of this policy is to establish rules for the backup of college computer systems and storage of backup media.

SCOPE

This policy applies to all computer systems that are supported and directly controlled by the KGRCET Information Technology Admin Department.

DESKTOP AND LAPTOP BACKUP POLICY

Local documents stored on desktop and laptop computers should be backed up so the documents and files can be restored in the event of a physical problem with the machine or if individual files or folders are inadvertently removed.

SERVER BACKUP POLICY

Backup procedures and policies are developed for two purposes, disaster recovery and file recovery. In the event of a catastrophe, due to a physical disaster, personnel error, or other misfortune, reliable backups must provide timely and accurate restoration of all functions of the organization. Individual file recovery may be required to restore programs, information or other data that has become corrupted or inadvertently removed.

6. COLLEGE MANAGEMENT SOFTWARE (CMS)

CMS is a comprehensive, fully-scalable campus information system or administrative platform designed specifically for use in Higher Education.

CMS allows your administrative and academic staff to access, update, store, and report on crucial data through a common database and a complete suite of end-to-end, fully integrated modules. Authorized users share real-time information across departments, streamlining workflow and optimizing business processes. KGRCET has The following CMS modules:

HOD Information Module

- Faculty Registration
- Subject Allocation

Faculty Information Module

- Attendance of students
- Mentoring of students

Student Information Modules

- Admissions
- Registration

LIBRARY SOLUTIONS

A server based JAVA driven library automation system that is connected to a web based Library Web Portal that included a Public Access Catalog. The system includes a workstation client for Circulation, Cataloging, and reporting.

NEWGENLIB

NewGenLib is an integrated library management system developed by Verus Solutions Pvt Ltd. Domain expertise is provided by Kesavan Institute of Information and Knowledge Management in Hyderabad, India.

NewGenLib version 1.0 was released in March 2005. On 9 January 2008, NewGenLib was declared free and open-source under GNU GPL.

The latest version of NewGenLib is 3.1.1 released on 16 April 2015. Many libraries across the globe (mainly from the developing countries) are using NewGenLib as

their Primary integrated library management system as seen from the NewGenlib discussion forum.

MODULES & FUNCTIONS

NewGenLib has following main modules:

- Acquisitions
- Technical Processing
- Serials management
- Circulation
- Administration
- MIS Reports
- Task to do today (daily scheduler)
- OPAC

Some advanced functional features:

1. Android mobile and tablet capable
2. Integration with Twitter helping send messages of transactions directly to users' Twitter accounts.
3. Flexibility of defining own search field in OPAC.
4. Enhanced contents and interactive OPAC like Availability of Book jackets, Google preview, Comments/ Book review, Tagging, Favorite reading list, etc.
5. Zotero compliant OPAC
6. RSS Feeds in OPAC
7. Faceted Browsing (Refining search results)
8. Suggestion for other books in the rack
9. RFID supports
10. Provision for frequently used predefined templates along with freedom of defining own customized data entry template s in Cataloguing
11. Configurable SMS system - a proof of transaction.
12. Integration with Gmail or paid mailbox account. This enables automatic sending of email to patrons during issue /return.
13. Enhanced Report Module for generating in .csv format with a provision for wide customization.
14. Provision for integrating with Vufind SOPAC (Ex: OPAC of the Library of Bangalore University).
15. Catalogue can be harvested through Google site map, and thus the visibility of the library can be further improved.

TECHNOLOGIES USED & STANDARDS SUPPORTED

NewGenLib uses a number of well supported and widely used, reliable and well tested open source components like PostgreSQL, Apache Tomcat, and Solr Lucene. It is entirely Java-based, platform-neutral, and uses the following major software technologies in its presentation, web server and database layers

- Java SE
- Apache Tomcat server
- Spring framework
- Hibernate framework
- Lucene and Solr
- JDOM for XML messaging
- Java Servlets, JavaServer Pages
- Java Mail
- OpenOffice.org for form letters
- JasperReports
- FreeMarker template (from version 3.04 R1)

NewGenLib is platform independent and can be installed on Linux and Windows operating systems.

SUPPORT FROM INFORMATION TECHNOLOGY ADMINS

The Information Technology Admin Department provides minimal to medium level support for this product; such as web programming, backup services, and workstation maintenance and updates. The Library Corporation provides the majority of support required through their Helpdesk.

7. KGRCET WEBSITE

The accuracy, timeliness, design, and speed (performance) of the web site are of strategic importance to the college since many external constituents view our web site.

DISCLAIMER

- All information provided in official KGRCET Web site is for information purposes only and does not constitute a legal contract between KGRCET and any person or entity unless otherwise specified.
- Information on official KGRCET web site is subject to change without prior notice.
- Although every reasonable effort is made to present current and accurate information, KGRCET makes no guarantees of any kind.
- The KGRCET web site may contain information that is created and maintained by a variety of sources both internal and external to KGRCET. These sites are un-moderated forums containing the personal opinions and other expressions of the persons who post the entries.
- KGRCET does not control, monitor or guarantee the information contained in these sites or information contained in links to other external web sites, and does not endorse any views expressed or products or services offered therein.
- In no event shall KGRCET be responsible or liable, directly or indirectly, for any damage or loss caused or alleged to be caused by or in connection with the use of or reliance on any such content, goods, or services available on or through any such site or resource.
- Any links to external Web sites and/or non-KGRCET information provided on college pages are provided as a courtesy. They should not be construed as an endorsement by KGRCET of the content or views of the linked materials.

STYLE GUIDELINES

The first several levels of the KGRCET web site are designed to project a consistent look in the use of headers, colors, fonts, and approaches to navigation. Site design standards are periodically reviewed and subject to change by the Director of Information Technology.

CONTENT GUIDELINE

The object of these guidelines is to insure that the content of KGRCET Web pages accurately represents KGRCET. All content must conform to the Acceptable Use Policies of KGRCET, language must be suitable to a public forum, content must be appropriate current and accurate, and external links monitored. Content should be non-discriminatory and protect individual privacy.

FORMAT GUIDELINE

- Spelling and grammar should be correct.
- HTML should meet W3C's Standards.
- Images should load correctly within a reasonable amount of time and include the ALT image tag parameter.
- All pages should utilize the KGRCET webpage template and be connected to the appropriate CSS style sheets for uniformity.

COPYRIGHT

- Copyright infringement is the illegal use of works under copyright, infringing the copyright holder's "exclusive rights", such as the right to reproduce, distribute, display or perform the copyrighted work, spread the information contained within copyrighted works, or to compose derived works.
- It frequently refers to copying "intellectual property" lacking written agreement from the copyright holder, which is normally a publisher or other business representing or assigned by the work's originator.
- Placing copyrighted material on the Web site without permission of the author is prohibited.

8. EQUIPMENT ACQUISITIONAND DISPOSAL

REPLACEMENT CYCLE

Most KGRCET computer equipment is replaced every three to five years to assure that appropriate computing resources are available in public and departmental computing facilities, classrooms, and KGRCET offices to support the mission ofthe institution; and implement minimum standards for computing equipment on campus; and also to encourage planning, cost-effective installation of new equipment and disposal of old equipment.

Computing equipment that is acquired under grants will enter the inventory and be upgraded on a regular replacement cycle *only* if approved at the time of the application for the grant.

PURCHASING

To ensure that technology purchases are compatible with existing campus systems, and can be supported by the Information Technology Admin Department, it is highly recommended that staff consult the Information Technology Director for all such purchases.

Information Technology Director will make final authorization prior to submission. Failure to comply may result in equipment that cannot be supported by the KGRCET Information Technology Admin Department.

RECOMMENDED COMPUTER SPECIFICATIONS (KGRCET COMPUTERS)

DESKTOP SYSTEMS

1. Operating System - Windows 7 Professional (Pre-Installed).
2. Operating System - Windows 7 Ultimate.
3. Minimum Intel Dual Core - Processor (1.9GHz).
4. 1-2 Gb Memory (Upgradable to 8Gb).
5. 160 Gb Hard-drive or greater.
6. Graphics Card - any with DVI support
7. DVD-RW
8. Monitor - 19" or larger LCD with DVI support.
9. USB Keyboard/Mouse Kit
10. 3-year Warranty

COMPUTER DEPLOYMENT, INVENTORY AND DELIVERY

All newly purchased computer workstations, laptops and servers shall be transferred to the Information Technology Admin Department after the item has been logged in the Business Office.

COMPUTER DEPLOYMENT

The Information Technology Admin department will install all supported software, enter into inventory, and deliver/set-up the computer to the required work area.

The Department is responsible for purchasing all peripheral items such as:

1. Computer desks ortables.
2. Keyboard/mouse.
3. Surge protectors.
4. Wireless or videocards.
5. Network switches.
6. UPS Battery Backupsystems.
7. Additional RAM orhard-drives.
8. Other.

INVENTORY

All computers, printers, and other devices to connect to the KGRCET LAN will be entered into the KGRCET Information Technology Admin Department Inventory System. The following information should accompany any new item to be deployed by the Information Technology Admin Department:

- ✓ Date ofPurchase.
- ✓ Cost ofitem.
- ✓ Fund Code information.
- ✓ Warranty Information.
- ✓ Staff, Faculty office, or room to be set-up in.
- ✓ Additional software requirements

ASSETS DISPOSAL

PURPOSE

The purpose of this policy is to establish and define standards, procedures, and restrictions for the disposal of non-leased IT equipment in a legal, cost-effective manner.

KGRCET surplus or obsolete IT assets and resources (i.e. desktop computers, servers, databases, etc.) must be discarded according to legal requirements and environmental regulations through the appropriate external agents and KGRCET upgrade guidelines.

Therefore, all disposal procedures for retired IT assets must adhere to company-approved methods.

SCOPE

This policy applies to the proper disposal of all non-leased KGRCET IT hardware, including PCs, printers, handheld devices, servers, databases, hubs, switches, bridges, routers, and so on.

Company-owned surplus hardware, obsolete machines, and any equipment beyond reasonable repair or reuse are covered by this policy.

Where applicable, it is desirable to achieve some residual value of the IT asset in question through reselling, auctioning, donation, or reassignment to a less-critical function.

DEFINITIONS

1. "***Non-leased***" refers to any and all IT assets that are the sole property of KGRCET; that is, equipment that is not rented, leased, or borrowed from a third-party supplier or partner company.

2. "***Disposal***" refers to the reselling, reassignment, recycling, donating, or throwing out of IT equipment through responsible, ethical, and environmentally sound means.

3. "***Obsolete***" refers to any and all equipment over 10 years old and/or that which no longer meets requisite functionality.

4. "***Surplus***" refers to hardware that has been replaced by upgraded equipment or is superfluous to existing requirements.

5. "***Beyond reasonable repair***" refers to any and all equipment whose condition requires fixing or refurbishing that is likely cost equal to or more than total replacement.

GUIDELINES

- Disposal and disposal procedures of all IT assets and equipment will be centrally managed and coordinated by KGRCET Information Technology Admin Department.
- KGRCET Information Technology Admin Department is also responsible for backing up and then wiping clean of company data all IT assets slated for disposal, as well as the removal of company tags and/or identifying labels.
- The IT Department is in charge of selecting and approving external agents for recycling hardware and/or sanitizing hardware of harmful toxins before shipment to landfills.

PRACTICES

Acceptable methods for the disposal of IT assets are as follows:

a. Sold to existing staff.
b. Donated to students.
c. Sold as scrap to a licensed dealer.
d. Used as a trade-in against cost of replacement item.
e. Reassigned to a less-critical business operation function.
f. Donated to schools, charities, and other non-profit organizations.
g. Recycled and/or refurbished to leverage further use (within limits of reasonable repair).
h. Discarded as rubbish in a landfill after sanitized of toxic materials by approved service provider.

POLICY

It is the responsibility of any employee of the KGRCET Information Technology Admin Department with the appropriate authority to ensure that IT assets, equipment, and hardware are disposed of according to one or more of the methods prescribed above.

It is imperative that any disposals performed by KGRCET are done appropriately, responsibly, and ethically, as well as with company resource planning in mind.

The following rules must therefore be observed:

1. **Obsolete IT Assets:** As prescribed above, “obsolete” refers to any and all computer or computer-related equipment over 10 years old and/or equipment that no longer meets requisite functionality.

2. Identifying and classifying IT assets as obsolete is the sole province of KGRCET’s IT Department. Decisions on this matter will be made according to KGRCET purchasing/procurement strategies.

3. Equipment lifecycles are to be determined by IT asset management best practices (i.e. total cost of ownership, required upgrades, etc.).

9. ENTERPRISE SERVER ROOMS AND NETWORK CLOSETS

PURPOSE

The purpose of this policy is to ensure a minimum level of security is maintained by all College staff that has access to the KGRCET Server Rooms.

SCOPE

This policy applies to all College Information Technology resources and Personnel who access those resources. It pertains especially to those resources that support critical enterprise systems.

POLICY

It is the policy of KGRCET to maintain an IT security program that protects the integrity, confidentiality, and availability of information resources, as well as addresses compliance with all applicable laws and regulations.

PHYSICAL ACCESS

The primary mechanism for controlling access to server rooms is a mechanical lock. Only Information Technology Admin Department staff shall be permitted in the server rooms unescorted.

All other visitors shall be escorted by Information Technology Admin Dept. staff. The Information Technology Director shall be notified of all server room visitors. KGRCET recognizes the responsibility for promoting an open computing environment.

CLIMATE CONTROL

General recommendations suggest that you should not go below 10°C (50°F) or above 28°C (82°F). Although this seems a wide range these are the extremes and it is far more common to keep the ambient temperature around 20-21°C (68-71°F).

- Information Technology Admin Department staff shall monitor server room temperatures and notify the Maintenance Department if the room temperature rises above 72 degrees.
- If Maintenance Department has exhausted local remedies, and needs to bring in third party support: The Information Technology Admin Department will take need measures such as powering off non-essential servers and other equipment. Additional fans may be used to circulate air. Critical services include KGRCET network domain controllers, primary DNS server, web server, and active director/e-mail services.
- If temperatures rise above 80 degrees, the Information Technology Admin Department will notify the Director of Information Technology Department, and give all staff and students 30 minutes notice viae-mail of the pending shut- down. Notice of Network Services downtime will be posted at the entry points to the college and college social media.

VIDEO SECURITY

Entry points to critical server and network closets shall be monitored and recorded by the campus video security system.

SERVER RACK GUIDELINES

The following guidelines have been established to guide installation of new equipment to the campus server racks.

9.7.1 POWER

Systems with redundant power supplies must have their power cords plugged into separate power strips. Power must be isolated from data cables.

9.7,2 RACK SPACE

Severs must be installed from the bottom up in the rack enclosures. Equipment must be clearly labeled.

9.7.3 DATA CONNECTIONS

Patch Cables must not exceed required length by more than one foot. All Fiber connections must not exceed a minimum bend radius as specified by the manufacturer. All Data connections must be clearly labeled.

10. COMPUTER WORK STATION SECURITY POLICY

PURPOSE

This Policy identifies KGRCET's procedures for ensuring that computers connected to the KGRCET are managed in a secure manner.

SCOPE

KGRCET has distributed computing environment with local responsibilities for the maintenance of computer security.

This security policy applies to networked computers owned or managed by KGRCET that contain information or allow access to information that is confidential under law or policy.

POLICY

To maximize the security of computers connected to the KGRCET network:

- ✓ All computers are required to have a user password at startup.
- ✓ All authorized users of KGRCET network resources are required to "Lock Down" (or log out) of the computer each time the computer is left unattended. If you are unsure how to Lock Down (or log out) of your computer, contact the Information Technology Help Desk.
- ✓ Individual user sessions must also initiate a password protected screensaver after a period of no more than thirty (30) minutes of inactivity. A shorter period of inactivity may be implemented at the direction of a department head.
- ✓ All authorized users of KGRCET network resources are required to follow the strong password characteristics and management practices. Whenever possible, passwords should be 8 or more characters long, and include letters, numbers, and punctuation characters. They should not be names, words in dictionaries, or permutations of personal data (birth dates or anniversaries etc.). Passwords should be changed periodically.
- ✓ Computers must contain –up-to-date antivirus software to ensure that files saved to them are not infected.
- ✓ Workstations should have installed the latest system updates and patches.

11. ENFORCEMENT

- ✓ Employee violations of any part of this policy will result in disciplinary action up to and including dismissal.
- ✓ Student violations of any part of this policy will result in disciplinary action upto and including suspension or expulsion.
- ✓ Authorized access to networks, systems, data, and information is a privilege grant to individuals to perform their KGRCET duties.
- ✓ Misuse of this access could result in the loss of this privilege and therefore the inability to perform one's job.
- ✓ By using KGRCET computing systems and signing the Appropriate Use statement users signify understanding and acceptance of the policies outlined therein.

PRINCIPAL
KG Reddy College of Engineering & Technology
Chilkur(V), Moinabad (M),
R.R. Dist. Telangana.