कर्नाटक केन्द्रीय विश्वविद्यालय

विद्या ददाति विनयम्

ಕರ್ನಾಟಕ ಕೇಂದ್ರೀಯ ವಿಶ್ವವಿದ್ಯಾಲಯ

Central University of Karnataka

Kadaganchi, Aland Road, KALABURAGI

CUK IT POLICIES AND GUIDELINES

TABLE OF CONTENT

Central University of Karnataka

IT Policies and Guidelines

1. Preamble

Central University of Karnataka (CUK), Kalaburagi is one among the Central Universities established under the act of parliament in the year 2009. Kalaburagi is one of the district headquarters located nearly 625 Kilometers away from the state capital Bangalore. The university comes under Kalyana Karnataka (Formerly Hyderabad Karnataka) region. The campus as of now has a network facility with NKN's 1 Gbps internet connectivity under NMEICT.

Since its establishment the University steadily found its growth in all sectors including the IT infrastructure and services sector. The University makes best use of IT, including hardware, software and services, for its routine activities.

Since from the time of its establishment the University realized that the IT infrastructure and internet are very vital for the growth. The IT products such as Computers, Printers, networking equipment, LCD devices, etc. were procured based on the needs arising for academic and office activities. The University became member of NKN (National Knowledge Network) sponsored by the Ministry of Human Development, Government of India, which provided the internet connectivity of 1 GBPS speed through its backbone across the country. This facility not only provides high speed internet connectivity to the students, research scholars and staff members of the University, but also provides abundant information resource needed for the students and research scholars.

Central University of Karnataka has different Schools, with interrelated departments within each school. Many school have the computing centres with internet connectivity. Individual schools are connected to the centralized network. The administrative departments are also connected to this network.

To further facilitate, University procured its own domain name and hosted the own website www.cuk.ac.in. Under the Google Apps for Education all the students including students and staff members got institutional email IDs. This was a part of University's policy of speedy delivery of information to the students of the institution.

With the increase in the number of users, the complexity also got increased. The vital resource like internet being used in uncontrolled manner may have the direct impact on the performance of internet because of the following reasons:

i. With no control on internet usage the prioritization of tasks does not happen. For example the tasks such as downloading of large files by a student and uploading of very important examination data will get same priority. This will hamper the high priority activities of the institution.

ii. Certain user(s) can misuse the resource affecting the critical users and applications.

iii. Since all the systems are interconnected, without any proper control an unauthorized user may creep into the privacy of other users and access the information from the computers of other users.

iv. Due to the interconnectivity, virus can spread from one system to other system.

v. The computer, IT hardware and software purchased may not be competent enough due to lack of proper analysis and study carried out before procurement.

The other constraints that may affect the users across the University, in particular the students and staff are:

i. Limited capacity of internet bandwidth.

ii. Limited and absolute resources such as computers, printers, IT laboratories, and other IT hardware and software.

iii. Limited financial resources allocated to the IT hardware, software and services.

iv. Limited availability of experts in specific software and IT services.

Realizing the above drawbacks the University took a decision to come out with a comprehensive IT policy, which could take into account all the above listed problems and constraints and would provide a viable solution to its users. The IT policy will broadly provide guidelines for procurement and usage of university's IT infrastructure and computing facilities including computer hardware, peripherals, software, institutional email IDs, information resources, intranet and Internet accessibility, which are collectively called "Information Technology (IT)". In view of these observations this document attempts to provide the IT policies and guidelines which would be relevant to this University.

Further, due to frequent changes and updates occurring in the Information Technology and information security sector, the policy governing information technology and information security should also need frequent changes and updates in its content, so as to fulfil the current requirements. Hence, the IT policy need to be reviewed on a regular basis and modified to reflect changing technology, changing requirements of the IT user community, and operating procedures.

This IT policy document will provide information regarding IT related activities and act as a guide to conduct acceptable actions and prohibits the violation of any defined activities. These guidelines are supposed to be used by all the stakeholders namely, students, research scholars, teaching faculty, non-teaching staff and any such person who is part of Central University of Karnataka. The IT policy is further subdivided in to following:

- ICT Service Management
- ICT Service Support for Hardware and Software
- Digital Information Security
- Network/Wi-Fi Security
- Email Security
- IT policy for website and its maintenance

The University IT Policy is applicable to all the entities and stake holders namely, centralized or individual administration of the IT technology, to all those administrative offices and departments who provide information services, the individuals who are the part of this University, provided by the university administration, school and departments, the authorized resident or non-resident visitors who use or connect to the University network using their own hardware. This IT policy also applies to the resources administered by the central administrative departments such as Library, Computer Centres, Laboratories, Offices of the University, hostels and guest houses, or residences wherever the network facility was provided by the University.

Further, the faculty, students, staff, departments, authorized visitors/visiting faculty and others who have permission to use the University's information technology infrastructure, must comply with the IT Policy and Guidelines. Any violations of IT policy defined in the IT policy document by any university member may result in disciplinary action. If the matter involves unlawful activity, then it may attract the legal action.

2. Computer Lab/Network Facility Centre

The University Computer Lab is responsible for monitor, support, maintenance and security of Information Technology infrastructure of the University. Besides these, the Computer Lab maintains and updates the official Website of the University and provides all the ICT related data supports in solving IT related problems. Also, it provides complete web service support for the online activities. Computer Labs provides various Technical services to Faculty members, staffs, and students of the University. It also provides support for Open-Source technologies and implementations and encourages their use in the University activities. Computer Lab provides the requisite IT services like Network, Internet, LAN and Wi-Fi facilities for the growth and development of Teaching, Learning, Research and Administrative activities of the University.

3. ICT SERVICE MANAGEMENT:

Computer Lab provides seamless and hassle-free access to ICT resources and services to the Central University of Karnataka Students and Staff community. The Computer Lab supports all computer-related equipment in use by faculty and staff on the Central University of Karnataka campus. All standard desktop computers and Laptops purchased through Procurement Section and configured by ICT staff receive full support. Full support is also provided for departmental network-connected printers. Every effort is made to respond to all requests for help but the level of support may be limited for some computers and peripherals, depending on their hardware configuration, software configuration, function, age or other factors. The ICT Team's approach is to take a proactive role and work with the university departments and individual faculty and staff members to make sure that the equipment purchased is supportable and ensure, through proper maintenance, that it continues to function reliably for its expected life span.

4. Methodology followed for ICT service support

- The IT team provides the first level of support for ICT problems. If possible, these will be done on-site, otherwise the equipment will be brought to the Computer Lab. If the problem persists, an outside vendor will be called to make the repairs.
- The IT team will utilize remote control tools when appropriate to provide quick problem resolution (the user's permission is required for remote control access).
- Requests are handled during normal working hours on weekdays.

- Requests will be prioritized according to urgency and number of users affected. Problems affecting an entire department (i.e. the inability to connect to the network or access a departmental printer) will usually take higher priority over individual problems. Non-operational computers will receive a higher priority than machines which are experiencing non-critical or intermittent problems. Computer viruses are given high priority because of their destructive potential and ability to infect other computers. Requests of approximately the same urgency will be handled on a first-come-first-served basis.
- If the requestor indicates that problems still exist or that additional assistance is needed in this matter, the IT team will continue working on the problem. If new, unrelated problems have occurred, the user should submit a new request.

5. Service support to ICT hardware

The IT team will respond to all requests for assistance and evaluate the nature of the problem. Most problems can be corrected on site, including simple hardware replacements, software installation, upgrades, or re-configuration. In more complex cases, the specialist may consult with IT team.

The comprehensive Annual Maintenance Contract (AMC) needs to be provided for the proper services to the University.

6. Service support to ICT Software

As with hardware, when the software installed on a computer is out of date, servicing becomes more difficult and time consuming. Beyond a certain point, technical assistance can no longer be obtained from vendors, compatibility problems arise, and familiarity of the IT team with the software diminishes. In order to comply with software licensing regulations, IT team will install only legally licensed software, freeware, or shareware.

As software companies release newer versions of software, the old versions eventually become obsolete for the following reasons:

- The software vendor no longer offers technical support for problems encountered
- The files or documents created by the software may be in a format no longer recognized by current software, making them un-sharable
- The original disks from which the software was installed may have been damaged or corrupted and can no longer be replaced.
- The software will no longer run under current computer operating systems

The IT Team does not support software that falls into these categories. If a user or department needs assistance with such software, the IT team will recommend a currently supported software package that will perform the required functions and assist the user in making the transition to the updated/new software.

IT team support all current versions Microsoft Windows/Mac OS/ Linux operating systems. The IT team will provide support for legacy/Mainframe software which is required for research purposes on a best-effort basis with support from external experts. The requirement of these software shall be certified by the concerned Project Investigator/Head of the Department concerned.

7. Backup of Desktop Data

In case the employee gets a new computer or hard drive replacement, the University will not be responsible for the restoration of data. It is recommended that the users of a computer make frequent data backups as and when needed.

8. DIGITAL INFORMATION SECURITY

Digital information is a vital asset to any organization, especially in a knowledge-driven organization, such as Central University of Karnataka. This clause mainly deals with the management and security of critical/confidential/personally identifiable information (PII) which includes (i) preventing unauthorized access, (ii) dealing with cyber-attacks and malicious software (like virus, Trojan horse, worm etc.) and (iii) misuse of ICT resources and services.

8.1 Information security implementation

Information security is implemented in the University through its technical controls (ie. administrative access controls to IT related facilities), firewalls, anti – malwares and backups of servers. The ICT team will ensure that the latest updated security patches are always available. ICT team shall conduct periodic inspection of all IT related facilities to ensure security related compliance. IT wing shall co-ordinate with departmental Heads and Deans for implementing technical access controls.

The secure individual username and password combination for every service (ie. email, internet, Wi-Fi, access to servers) is provided by the University. It shall not be shared with other users. The users are responsible for the activities from their respective login account. Each common computer/device in department is secured with an administrative username and password which is known only to the concerned departmental Computer Lab Coordinators.

However computers used by other faculty members or used in the Labs/Offices of other faculty members are exempt from this.

Currently there is no security classification for digital information. But it may be implemented, if needed, in future and the policy may be amended with suitable clause and procedures for the same.

8.2 Data retention Policy

In order to ensure that the critical data of Central University of Karnataka is backed up regularly, the following important precautions shall be followed for minimizing risk by ICT team.

- Website data is backed up periodically.
- Periodic backup from different servers that are used for specific functions.
- RAID to be configured on servers
- Data to be backed up in a separate Backup server
- Servers to be configured in DMZ

University currently do not have provision to provide server storage space to users. It will be enabled in the future based on the availability of the server storage space. In such cases, if the user request for space, based on availability, it will be provided to the user. Such space so allocated should not be used to store copies of personal photographs, music collections, etc. Multimedia documents stored for academic purposes are exempt from this clause.

8.3 Data Classification Policy

Central University of Karnataka will classify its data under the following heads.

- **Confidential**

  Any digital data which has to be protected from public/internal access which can result in legal ramifications (Eg:- Recruitment Data, E-Filing Data, Tendering Data, Student/Staff Personal Information) may be classified as confidential. This data shall be strictly protected with all access control measures to ensure that only concerned people have access to the data.

- **Internal-Only**

  Digital Data which is required for conducting the day-to-day business of the University which will be processed and accessed by various staff shall use the Internal-Only Label. However, these details may be limited to access only to staff who has to process such data. (E.g.:- Leave Details, Salary Details, Emails, Program Recordings, etc.)

- **Public**

Any data which has to be made publicly available through website/data coming under RTI shall be considered under public classification.

8.4 Data retention Policy related to Meeting Recordings

The ownership of the video recordings of the meeting like Executive Council/Finance Committee/Court Meetings/Other Seminars/Conferences will be with the Organizing Secretary/ of the concerned meetings. ICT team will only act as the facilitator of the recordings/meetings.

9. NETWORK/WI-FI SECUIRTY

9.1 Authentication methods

Security is implemented using authentication services like Firewalls, RADIUS/LDAP Authentication/ Wireless Access Point Authentication based on WPA/PSK2.

Issuance of an account to a system user is given by the Computer Lab of Central University. The Username and password combinations are generated and controlled by Authentication based on AAA (Authentication, Authorization and Accounting) procedures.

User will be held responsible for any misuse of account. Maximum Number of Concurrent (simultaneous) logins for a user account is limited to two devices of user choice.

9.2 Wi-Fi Network Security

Wi-Fi network access will be provided on a best effort basis to all desired locations including class rooms, seminar halls and locations frequented by faculty and students.

Any wireless network device that would extend the University network used by user and is not managed by the Computer Lab must be intimated. If Computer Lab finds out any device which is utilized as rogue device, it will be subject to detection and immediate removal from the network. The access points provided in the campus are the property of University and any damage or loss of the equipment will be considered as a serious breach of University's code of conduct and disciplinary action will be initiated on the student/faculty who found guilty for the loss or damage of the Wireless Infrastructure or the equipment in the campus.

10. MOBILE DEVICE USAGE POLICY

10.1 Definition of Mobile Device

As mobile devices further incorporate features traditionally found in a personal computer, their smaller size and affordability make these devices a valuable tool in a wide variety of applications. However, these devices are also subject to increased risk of loss, theft, and unauthorized use.

10.2 Purpose

The standards are established based on configurations and management guidelines for mobile computing devices (e.g., cellular or smart phones, laptops, tablets, etc.) owned and/or operated by the Central University of Karnataka or its workforce. As there are a wide variety of mobile device operating systems, software, and system configurations used across the University, this document is NOT intended to be a definitive and comprehensive guide to device security.

Compliance with these standards does not exempt a device from meeting union, state, or local laws and regulations. For example, if the device is collecting or storing credit card data, then the application and server must comply with all Payment Card Industry (PCI) standards.

Effective implementation of these standards will minimize the likelihood of unauthorized access to University computing resources and legally restricted and/or confidential information. All security events (e.g., loss of, or unauthorized access to device) must be reported to the appropriate personnel as soon as they are discovered, in order to ensure compliance with legal obligations.

10.3 Requirements

Physical Protection: Individuals must keep mobile devices with them at all times or store them in a secure location when not in use.

Password Protection: Access to the mobile device must be protected by the use of a password.

Encryption: University data classified as confidential must not be stored on a storage card or the device (including within cached email) without proper encryption, password protection and inactivity timeout.

Inactivity Time-out Protection: Inactivity timeout must be set. The recommended inactivity timeout is 5 minutes but must not exceed 60 minutes.

Proper Disposal: Any residual settings, data, and applications on the mobile device must be removed or wiped prior to disposal or transfer to another user. All attached storage cards that contain personal Information must be destroyed or wiped so no data recovery is possible.

Lost or Stolen Device: If a mobile device containing University information is lost or stolen, report the loss immediately to The Registrar, Central University of Karnataka. They will initiate necessary action to protective/corrective action. In addition, the incident must also be reported immediately to the Police Station.

10.4 Additional Recommendations for Mobile Devices

Invalid Password Attempts: The device should be set to lock after 10 invalid password attempts.

Disabling Unused Services: Wireless, infrared, Bluetooth or other connection features should be turned off when not in use.

Remote Configuring Capability: The mobile device should support the ability to remotely reset the device, including the deletion of all locally stored data.

11. Internet Usage Policy:

- Internet is a paid resource and therefore shall be used only for Academic, Research and office work.
- The organization reserves the right to monitor, examine, block or delete any/all incoming or outgoing internet connections on the organization's network.
- The university has systems in place to monitor and record all Internet usage on the university network. The ICT team can choose to analyze Internet usage and publicize the data at any time to assure Internet usage is as per the IT Policy.
- The university has installed an Internet Firewall to assure safety and security of the organizational network. Any employee who attempts to disable, defeat or circumvent the Firewall will be subject to strict disciplinary action.

11.1 Internet Login Guidelines

- All employees and students are provided with a User ID and Password to login to the Internet network in the university campus and to monitor their individual usage.
- All employees and students are responsible for the internet usage and user id and password.

- User ID and password for a new employee must be requested through application available over intranet. Printed Application forwarded by HoD/Section head needs to be submitted to Network Facility Centre for creation of Internet usage credentials.
- Sharing the User ID and Password with another employee, Students, visitor or guest user is prohibited.
- A visitor or guest user who wants to use the office Internet will be given a Guest User ID and Password.
- The ICT Team/NFC section shall define guidelines for issuing new passwords or allowing employees to modify their own passwords.
- Any password security breach must be notified to the Network Facility Center/Computer Center/ICT Team immediately.
- User ID and password allotted to an employee and Students will be deleted upon Completion of course /resignation/termination/retirement from the university.

12. EMAIL USAGE GUIDELINES

Electronic mail (email) with domain **@cuk.ac.in** is a primary means of communication both within the CUK and externally. It allows quick and efficient conduct of digital communication, but if used carelessly or illegally, it carries the risk of harm to the University and members of its community.

12.1 Eligibility for official Email-id

The eligibility criteria for official email access is as following:

- Can be issued to all permanent staffs irrespective of their cadre.
- Students will be issued email authentication credentials on the request of the concerned HoDs. General format for the email ids for students should be as follows: "roll.no/registration no."@cuk.ac.in.

12.2 Email service

Email services are primarily intended to allow faculty and staff to conduct University Academic and Research activities. Personal use of email is allowed, provided that personal use (a) does not materially interfere with performance of work responsibilities, (b) does not interfere with the performance of the University networks.

The University also reserves the right to inspect or check the access email accounts and contents with this policy in extreme cases, and to take such other actions as in its sole discretion it deems necessary to protect interests of the University based on approval of higher authorities. The University further reserves the right to enforce these provisions with or without prior notice to the user.

12.3 Email maintenance

Central University of Karnataka is having Google Education subscription for email service. Hence loss of email content is not the responsibility of the University.

The official email ids of employees of the University will be deactivated within three months form the date of leaving Central University of Karnataka. In the case of students/research scholars it will be deactivated within one week after the declaration of the result of the final semester.

The E-mail address of the faculties relieved/retired from the University and PhD scholars who pass out of the University may be permitted to retain up to one year based on the recommendation from the concerned head of the department.

13. Email Security

13.1 Safe Email Usage: Following precautions must be taken to maintain email security:

- Do not open emails and/or attachments from unknown or suspicious sources unless anticipated by you.
- In case of doubts about emails/ attachments from known senders, confirm from them about the legitimacy of the email/attachment.
- Use Email spam filters to filter out spam emails.

14 Installation and Maintenance of Software

The software register should include the following information (as a minimum):

- Name of the software.
- Software vendor's name.
- Date of purchase and installation.
- Purchase cost.
- Purchase order no, invoice number and date.
- Name of the authorized user(s) or installation location.
- A list of the associated documents/manuals and their location. In particular, this item should reference the location of the original software media and the license agreement document consisting of serial number (software key) of the software (where applicable).
- software agreement expiry date (if applicable) / renewal date (if applicable)

All purchase related documents including the original media, license documents, manuals and other associated material must be maintained in the concerned sections for formal audits or license checks.

15 Software Usage Policy

- Third-party software (free as well as purchased) required for day-to-day work will be preinstalled onto all systems before handing them over to employees. A designated person in the Network Facility Centre/Computer Centre can be contacted to add to/delete from the list of pre-installed software on computers.
- No other third-party software – free or licensed can be installed onto a computer system owned without prior approval of the Network Facility Centre/Computer Centre.
- To request installation of software onto an official computing device, an employee needs to send a written request via Email.

- Any software developed & copyrighted by the organization belongs to the organization. Any unauthorized use, storage, duplication or distribution of such software is illegal and subject to strict disciplinary action.

16 Compliance

- All employees and students are expected to comply with the IT Policy rules and guidelines while purchasing, using and maintaining any equipment or software purchased or provided by the CUK.
- Any employee who notices misuse or improper use of equipment or software within the CUK must inform his/her Reporting Network facility Centre/Computer Lab immediately.
- Inappropriate use of equipment and software by an employee will be subject to disciplinary action as deemed fit by the IT Committee of the CUK.

17 IT policy for website

University is actively using IT resources like websites, email services, social sites, short messaging services and other electronic communication systems for communicating and interacting with the users of the system. These types of communications have potentially reduced the cost incurred by institution and speeded the communication. Since most of the users would be dependent on the information provided through these communications, effectively maintaining and updating the information on websites would be one of the duties of the University.

18 Policy for website and content developers

Web developers are the one who have the skill of website development and involved in the development of University website. They will be responsible for design of the overall website, creating the web content structure, organization of its content, adding graphics and images during its design, writing codes for its background functionalities, providing rich features to the website etc. The web content developers may be external agencies hired by the University for One Time Development. University may get extended their services whenever there is need for revision or modification in the website design.

The primary aim of the web developers must be to provide a stable website as per the requirements of users. They are supposed to use the latest secure and standard high end languages and database during the development of website. The orientation must be for using open source scripting tools and databases. The hosting of website over the servers should not attract additional cost on the University such as cost involved in purchasing website development tool or database tool. The designers should not use unsecure database files such as Excel sheets or flat files for storage and retrieval of data. The scripts not related to the website such as batch scripts, other processes, any other applications not related to website and not used by the Central University of Karnataka should not exist on the web server. The database applications required by departments/schools may be uploaded with permission from the higher authority.

19 Policy for website administrators

Website administrator is employee of Central University of Karnataka whose role will be to manage entire website. Website administrator manages the operational component of website. The web operations are providing access to website, verifying the content of the website to check for up- to-date content in it, and any such related operations.

In emergency situations like hacking, breakdown or attack on website, the website administrator must be able to effectively and rapidly replace the website with the message stating non-availability of website for temporary reasons or redirect them to some other website. The website administrator must also be able to change, disable, activate, deactivate, delete, add any website content as and when any such request comes from the higher authority.

Website administrator should follow proper naming convention for the files, images, and other web contents which would be uploaded into the website. He/she should also be able to give proper identification code or login details for every website contributors with proper authentication procedure. Website administrators should monitor website content to ensure appropriate use and compliance with IT policy and ensure that Web developers and content contributors at all levels follow all policies as described in the previous sections.

20 Other policy guidelines related to website

Web media is the content such as audio, video, multimedia files and other file types excluding the web pages. Web media files are usually very large in the size and require more storage space and higher bandwidth for uploading and downloading. Because its large usage of internet resource some guidelines are described in this section to manage web media content in website. The department/School/section heads, in consultation with their subordinates must plan for maintaining rich multimedia content in their gallery. Such media content may be photographs, short videos, audios, etc. Before uploading such content proper approval must be obtained from the higher authority.

Streaming and delivery of any Web media on the University network will be monitored and fine-tuned to ensure reliable content delivery based on the capabilities of the existing network infrastructure. Needs for system specifications, network and bandwidth information can be communicated in advance to the IT department so as to make appropriate arrangement for smooth streaming of event.

21 Responsibilities of Network Facility Centre/Computer Lab.

The Network Facility Centre/ Computer Lab of University will consist of a senior IT head having overall expertise of hardware, software, network and internet. He/she will be assisted by Team of IT assistants who could implement the plans and instructions given by the IT head. The IT department will have all tools and machines required for extension works, troubleshooting and maintenance of campus IT products such as hardware devices, peripherals, software tools, local area network and internet.

- **Management of Campus Network Backbone:** The campus network once established, will interconnect all the departments/schools with the centralized resources such as servers, databases etc. Network Facility Centre/Computer Lab will be responsible for smooth functioning of this network backbone.
- **Logical and physical separation of departments:** For the purpose of optimal utilization of network resources such as OFC networks, bandwidth, routers etc the IT department has responsibility to logically and physically divide these resources optimally among different departments/Schools depending on the number of users. The IT department will have to provide justice to everyone in making provision for internet resources. They have to see to it that everyone get fair bandwidth and wherever there is need for excessive bandwidth, proper arrangements need to be made by fairly looking into the requirements. The IT department will also be responsible for the planning and executing the extended cabling in campus and within the buildings.
- **IP address allocation:** IP addresses are one of the scarce resources which need more attention in allocation. If the genuine request comes for static IP addresses, same may be allocated by obtaining approval from the higher authority. NAT addressing can be used for providing enough IP addresses to the departments/schools. While allocating IP addresses the future requirements of the Departments/Schools has to be considered and accordingly the provisions should be

made.

- **Activity monitoring:** Network Facility Centre/Computer Lab will be responsible to keep watch on the activities happening across entire campus network using appropriate firewall software. The monitoring can be made on activities like checking unauthorized users, sending spam mails by users, downloading and uploading unusually large size files, visiting the harmful and adult websites, skewed usage of internet bandwidth, unauthorized access to University database, hackers of University website, etc. If any of the above activity found then necessary action must be taken to prevent further activity and details of activity must be reported to higher authority for further disciplinary action. The Network Facility Centre/Computer Lab department will not have authority to open any users' email addresses or access any users' emails without users' permission.
- **Management of institutional email ID:** University employees and students extensively use the institutional email IDs for their regular communication. They are unequally identified globally by the institutional email IDs. Whenever a new user (employee or student) is added to the institution the Network Facility Centre/Computer Lab department must make provision for his/her email ID. Convention for creating email IDs must strictly be followed. Once email ID is created, its authorized user must be intimated and user must be forced to change the login password. When an employee leaves the organization or retires from service or dies, the email ID of such employee must be withdrawn. University Students and Staff should not misuse institutional email ID for their personal gain or with the intention to bring bad name to the institution.
- **Installation and management of wireless network:** In the current era of wireless communication, the usage of wireless devices such as smart phones, laptops and tablets are increasing day-by-day. On establishment of campus internet network, wireless internet facility must be made available to users who opt to use internet using their wireless devices. The usage must start with appropriate login process. At any instance any authorized user should not be able to login in more than two instances.
- **Renewal of licenses:** Network Facility Centre/Computer Lab department will be responsible for the renewal of any licenses, lease periods, warranty period of IT resources such as data servers and routers, domain name and domain space, etc.

related to the entire University campus. The renewal must happen before the expiry period. Before proceeding for any renewal permission must be obtained from the higher authority.

22 Responsibilities of University Departments/Schools

University Departments/Sections/Schools are the major users of the University IT resources. They play important role in the usage of IT resources. Following are the few guidelines for optimal utilization of IT resources by the users from these sectors:

- **IT resource management:** Every user/employee and head of respective department/School shall be responsible for maintenance of IT resources. If any device is found to be faulty same must be reported to the Network Facility Centre/Computer Lab to get it serviced. Proper stock register must be maintained for all the IT hardware devices and software tools. When any device is found to be unusable, same may be written off with approval from the higher authority. If any of the e-waste has to be disposed off, appropriate disposal methodology has to be followed to avoid the hazard in the environment.
- **Updating web content:** www.cuk.ac.in Website is logically divided based on the Departments/Schools/Sections. Every authorized user could login and update the information related to respective sections. The head of related Department must check the content before providing approval. Since the approval issue system is via email, care must be taken regarding the content of the matter to be uploaded into website.
- **Website Archives Data:** The Archives data available on the Website will be retained for a maximum period of Two Years or the data may be removed/updated at any time based on the directions of the University competent authority.
- **Internet resource usage:** Network Facility Centre/Computer Lab will be responsible for detailed monitoring of internet usage. Students and users must be instructed to avoid downloading of larger files, particularly the files not related to academic, research or their work. Users must also be instructed to avoid visiting the social network websites, chatting sites, news forums, entertainment, adult sites, etc. If anyone is found violating the instructions, appropriate action must be taken to suspend/withdraw the user login from such user.
- **IT infrastructure expansions:** Any Department/School willing to expand the IT infrastructure such as network, computer lab infrastructure, they

must bring same to the notice of Network Facility Centre/Computer Lab regarding proposed expansion activity. Such expansion should not affect the normal activities of other Departments/Schools and should not overburden the existing campus network/internet bandwidth. Unnecessary expansions must not be taken up by any Department/School.

- **Use of legal software/hardware:** The Department/School heads must strictly instruct the users not to use illegal/unlicensed software and hardware devices. Use of any software for hacking websites, hacking email IDs, steeling classified information from any website, steeling personal information of any individual, destroying the software set and operating system of the PCs, spreading viruses, sending spam emails, attacking the University servers, intentionally or unintentionally should be strictly prohibited. Any snooping device should not be installed.

23 Cyber Security Dos and Don'ts

Cyber security is the shared responsibility of every Students/Research Scholars/Staff of Central University of Karnataka. Users play a key role in properly safeguarding and using private, sensitive information and state resources. IT support will set up the network security defence configurations, it is up to each and every Student/Research Scholar/Staff to do their part in using the system safely.

The following Cyber security Dos and Don'ts help remind us of actions one must take to remain vigilant.

- **DO** use hard-to-guess passwords or passphrases. A password should have a minimum of 10 characters with the combination of uppercase letters, lowercase letters, numbers, and special characters. To make it easy for you to remember but hard for an attacker to guess and create an acronym.

- **DO** use different passwords for different accounts. If one password gets hacked, your other accounts are not compromised.

- **DO** keep your passwords or passphrases confidential. DON'T share them with others or write them down. You are responsible for all activities associated with your credentials.

- **DO** pay attention to phishing traps in email and watch for telltale signs of a scam. DON'T open mail or attachments from an untrusted source. If you receive a suspicious email, the best thing to do is to delete the message.
- **DO** destroy information properly when it is no longer needed. Place paper in designated confidential destruction bins throughout the office or use a crosscut shredder for all electronic storage media.

- **DO** be aware of your surroundings when printing, copying, faxing or discussing sensitive information. Pick up information from printers, copiers, or faxes in a timely manner.
- **DO** remember that wireless is inherently insecure. Avoid using public Wi-Fi hotspots. When you must, use agency provided virtual private network software to protect the data and the device.

- **DO** report all suspicious activity and cyber incidents to your manager and ISO/designated security representative. Challenge strangers whom you may encounter in the office. Keep all areas containing sensitive information physically secured and allow access by authorized individuals only. Part of your job is making sure NYS data is properly safeguarded, and is not damaged, lost or stolen.

- **DO** lock your computer and mobile phone when not in use. This protects data from unauthorized access and use.

☒ **DON'T** leave sensitive information lying around the office. DON'T leave printouts or portable media containing private information on your desk. Lock them in a drawer to reduce the risk of unauthorized disclosure.

☒ **DON'T** post any private or sensitive information, such as credit card numbers, passwords or other private information, on public sites, including social media sites, and DON'T send it through email unless authorized to do so. DO use privacy settings on social media sites to restrict access to your personal information.

☒ **DON'T** click on links from an unknown or untrusted source. Cyber attackers often use them to trick you into visiting malicious sites and downloading malware that can be used to steal data and damage networks.

☒ **DON'T** be tricked into giving away confidential information. It's easy for an unauthorized person to call and pretend to be an employee or business partner. DON'T respond to phone calls or emails requesting confidential data.

☒ **DON'T** install unauthorized programs on your work computer. Malicious applications often pose as legitimate software.

☒ **DON'T** plug in portable devices without permission from IT Department as these devices may be compromised with code just waiting to launch as soon as you plug them into a computer.

☒ **DON'T** leave devices unattended. Keep all mobile devices, such as laptops and cell phones physically secured. If a device is lost or stolen, report it immediately to your manager and ISO/designated security representative.

☒ **DON'T** leave wireless or Bluetooth turned on when not in use. Only do so when planning to use and only in a safe environment.

IT Team CUK is dedicated to protecting privacy; safeguarding the University information assets and infrastructure; identifying and mitigating vulnerabilities; detecting, responding, and recovering from cyber incidents; and promoting cyber awareness and education. Remember - cyber security is everyone's responsibility! All users take these are steps must take immediately.

CUK IT Policy Drafting Committee:

Following are the members of the CUK IT Policy Drafting Committee:

1. **Prof. Ravindra Hegadi**	-Chairperson, Prof. Dept. of Computer Science.
2. **Prof. Srikantaiah**	- Member, HoD, Dept. of Computer Science.
3. **Dr. Veeresh G K**	- Member, Associate Prof. Dept. of E & CE.
4. **Dr. Rajeev Joshi**	- Member, Associate Prof. Dept. of Physics.
5. **Mr. Vinodkumar T**	- Member-Convenor, System Analyst.

--- END ---