GENERAL SIR JOHN KOTELAWALA DEFENCE UNIVERSITY

POLICY ON

Information & Communication Technologies

Contents

1. Introduction

General Sir John Kotelawala Defence University (hereinafter referred as to KDU) was initially established as the "General Sir John Kotelawala Defence Academy" by the Parliamentary Act No 68 of 1981 and subsequently it was elevated to University status by the amendment Act No 27 of 1988, thereby empowering it to award Bachelors' and Postgraduate degrees in Defence Studies. KDU is a member of the Association of Commonwealth Universities (United Kingdom) and maintains necessary standards for educating and grooming Officer Cadets to meet the challenges of modern defence management. KDU is now open for civil students who wish to continue their higher studies in various disciplines.

General Sir John Kotelawala Defence University (KDU) provides IT resources to support the educational, instructional, research, and administrative activities of the university and to enhance the efficiency and productivity of the employees. These resources are meant as tools to access and process information related to their areas of work. These resources help them remain well informed and carry out their functions efficiently and effectively.

This document establishes specific requirements for the use of all IT resources at KDU. This policy applies to all users of computing resources owned or managed by KDU. Individuals covered by the policy include (but are not limited to) KDU faculty and visiting faculty, staff, students, alumni, guests, external individuals, organizations, departments, offices, affiliated colleges, and any other entity which falls under the management of General Sir John Kotelawala Defence University accessing network services via KDU's computing facilities.

The term 'IT Resources' includes all university owned, licensed, or managed hardware and software, and use of the university network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

The stakeholders of this policy must refer to the latest version of this document, and misuse of these resources can result in unwanted risks and liabilities for the university. It is, therefore, expected that these resources are used primarily for university related purposes and in a lawful and ethical way.

2. Scope

This policy governs the usage of IT Resources from an end user's perspective. This policy is applicable to all individuals/ users/ entities, as defined in Section 2, who use the IT Resources of KDU.

3. Aims and Objectives of the Policy

3.1 Aim

The policy on ICT aims to ensure proper access to and usage of KDU's IT resources and prevent their misuse by the users. Use of resources provided by KDU implies the user's agreement to be governed by this policy.

3.2 Objectives

The objectives of this policy are

- To maintain, secure, and ensure the legal and appropriate use of Information Technology infrastructure established by the university on the campus.
- To establish university-wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the university.
- To address all information assets, including data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information.

4. Principles and Values

1. This policy is applicable to all the users of KDU as specified in Section 2 of this document. It is mandatory for all users to adhere to the provisions of this policy.
2. Each entity of KDU shall be responsible for ensuring compliance with the provisions of this policy. The Implementing Agency (IA) would provide necessary technical assistance to the users who are entities in this regard.

5. Policy Statement

1. Acceptable Use

- An authorized user may use only the IT resources he/she has authorization. No user should use another individual's account or attempt to capture or guess other users' passwords.
- A user is individually responsible for appropriate use of all resources assigned to him/her, including the computer, the network address or port, software, and hardware. Therefore, he/she is accountable to the university for all use of such resources. As an authorized KDU user, he/she should not engage in or enable unauthorized users to access the network by using IT resources of KDU or a personal computer that is connected to the KDU campus wide Local Area Network (LAN).
- If the university is bound by its End User License Agreements (EULA), respecting certain third party resources; a user is expected to comply with all such agreements when using such resources.
- Users should make a reasonable effort to protect his/her passwords and to secure resources against unauthorized use or access.
- No user must attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.
- Users must comply with the policies and guidelines for any specific set of resources to which he/she have been granted access.
- When other policies are more restrictive than this policy, the more restrictive policy takes precedence.

2. Privacy and Personal Rights

- All users of the university's IT resources are expected to respect the privacy and personal rights of others.
- Do not access or copy another user's email, data, programs, or other files without authorization and approval of the Competent Authority (CA) who owns such components of information.

- While the university does not generally monitor or limit content of information transmitted on the campus wide LAN, it reserves the right to access and review such information under certain conditions after due approval of theCA.

3. Privacy in E-mail

While every effort is made to ensure the privacy of KDU email users, this may not always be possible. Since employees are granted use of electronic Information Systems and network services to conduct university activities, there may be instances when the university, based on approval from Competent Authority, reserves and retains the right to access and inspect stored information with the consent of the user.

4. User Compliance

When an individual uses KDU's IT resources, and accepts any university issued computing accounts, it means that the individual agrees to comply with this and all other computing related policies. It is the responsibility of the individual to keep oneself up-to-date on changes in the IT policy of KDU and adapt to those changes asnecessary from time to time.

5. Access to the Network

- Access to Internet and LAN

i. A user shall register the client system and obtain one-time approval from the CITS & DS before connecting the client system to the university's LAN.

ii. Users shall not undertake any activity through any website or applications to bypass filtering of the network or perform any other unlawful acts which may harm the network's performance or security.

- Access to KDU's Wireless Networks

For connecting to a KDU's wireless network, user shall ensure the following:

i. A user shall register the access device and obtain one-time approval from the competent authority before connecting the access device to the KDU's wireless network.

ii. Wireless client systems and wireless devices shall not be allowed to connect to the KDU's wireless access points without due authentication.

iii. To ensure information security, it is recommended that users should not connecttheir devices to unsecured wireless networks.

- Filtering and blocking of sites

i. CITS & DS or any other Implementing Agency (IA) nominated by the university may block content over the Internet which may pose a security threat to the network.

ii. CITS & DS or any other Implementing Agency (IA) nominated by the university may also block content which, in the opinion of the university, is inappropriate ormay adversely affect the productivity of the users.

6. Monitoring and Privacy

- CITS & DS or any other Implementing Agency (IA) nominated by the university shall have the right to audit networks and systems at regular intervals, from thepoint of compliance to this policy.
- For security related reasons or for compliance with applicable laws, IA may access, review, copy or delete any kind of electronic communication or files stored on university provided devices under intimation to the user. This includes items such as files, e-mails, posts on any electronic media, Internet history etc.
- IA may monitor user's online activities on university network, subject to such Standard Operating Procedures of Government of Sri Lanka (GoSL) norms.

7. E-mail Access from the University Network

- E-mail service authorized by KDU and implemented by the CITS & DS shall onlybe used for all official correspondence.
- More details in this regard are provided in the "E-mail Usage Policy of KDU".

8. Access to Social Media Sites from KDU Network

- User shall comply with all the applicable provisions under any existing

written and/or unwritten laws in Sri Lanka while posting any information on social networking sites.

- User shall adhere to the "Terms of Use" of the relevant social media platform/website, as well as copyright, privacy, defamation, contempt of court,discrimination, harassment, and other applicable laws.
- User shall report any suspicious incident as soon as possible to the Competent Authority of such content or to the IA.

- User shall not post any material that is offensive, threatening, obscene, infringes copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist,or is otherwise unlawful.
- User shall not disclose or use any confidential information obtained in theircapacity as an employee of the university.
- User shall not make any comment or post any material that might otherwisecause damage to KDU's reputation.

9. Use of Social Media

- KDU will be communicated via social media platforms, which will represent the university's broader values and culture. A coherent and recognizable portrayal of the university is of paramount importance because it will be easily identifiable as apart of the university.

- The university social media pages are the responsibility of the Director CITS &DS or their nominees.

- This includes the university's official social media sites, as well as university profile pages on third-party sites like Facebook, Twitter, LinkedIn, and YouTube.

- Third party sites (Facebook, Twitter, LinkedIn, and YouTube) are mainly design under the university and the associate pages are created for the faculties and the departments.

- The university's official web site will be used to share the articles/news of the

university community and to share the e books for the readers available in the library.

- Only the content provider (i.e., respective Deans/Directors of the department/division) may request through the Director CITD & DS to Web Coordinator of the university to set up an article/news in the respective web presence in the official web site of KDU only with the approval of the Deputy Vice Chancellor (Defence & Administration) .
- The Web Coordinator of each faculty/division may forward the articles/news to the Dean/Director or the Head of Section to be forwarded to the Director CITS& DS.
- Personal Accounts on Social Media Sites Users should use third-party social media sites like Facebook, Twitter, YouTube, and LinkedIn at their own risk. Since the university has no power over these pages, it cannot be held liable for any data stored on them.
- In addition to the rules outlined in this Policy, users should familiarize themselves with the terms and conditions that govern each social networking platform.
- While the KDU does not prohibit private use of social media, it is necessary to remember that the same professional standards, rules for communicating with students, alumni, the media, and other university constituents, and national laws apply online as they do in person. You are responsible for anything posted on yourpersonal social media sites.
- Users should protect themselves by reading and being familiar with the privacy policies regulating the social media platform to ensure that they support any data disclosures that might be made. It is strongly advised that users keep their privacysettings on such pages as high as possible (Ex. a private profile on Facebook)
- Think about what you're going to post before you do it. And after a user's social media account has been deactivated, copies of the user's details can still be available on the internet. As a result, users should think about the long-term online footprintthey are leaving before uploading content.

10. Social Media Content Access, Creation, and Sharing

- All requests for updates or new posts to a university's social media site must go through the Director CITS &DS and will be considered on a case-by-case basis.
- Accessing, creating, and sharing content related to the university and personal social media sites must comply with the Permitted and Prohibited Activities as specified in the University Acceptable Use Policy (AUP).
- Users are encouraged to use their department, division, or project social media platforms to communicate responsibly at all times, with due respect for the 'University' and 'others' rights and reputations, as described in the AUP.
- All university social media sites must identify themselves as members of the university administration.
- Each social media site must contain contact details of the department, division, or project, as well as an e-mail address that is regularly followed up by the web content creator or web coordinator. Web coordinator (or their nominee) is responsible for monitoring and maintaining the site and should check the sites/e-mails for new posts/comments at least once a week.
- Time calendar with news and events should be presented to the faculty board in every month and should get the approval before sending to the Director CITS &DS
- All messages posted by followers must be moderated before appearing on any university social media site. Any posts/comments that are illegal, obscene, defamatory, harassing, discriminatory, threatening, infringing on the intellectual property rights of others, an invasion of privacy, or violation of AUP must not be published.
- All university social media pages should meet the goals of high quality in both style and presentation. All social media sites must be regularly updated with at least one post per month. While the language used can fit the style of the particular social media platform, care must be taken to preserve the semantics of the message, and not to have obvious grammar and spelling errors.

11. E Learning

E –learning comprises all forms of electronically supported learning and teaching. E-learning is essentially the computer and network-enabled transfer of skills and knowledge. E-learning applications and processes include Web-based learning, computer-based learning, virtual

education opportunities and digital collaboration. Learner's access primary content and instruction from an e-learning environment using a variety of tools including, but not limited to, e-mail, text and voice chat, discussion boards, web pages, and multimedia technologies. KDU has implemented Learning Management System (LMS), remote learning facilities through the Lanka Education and Research Network (LEARN), Virtual Learning Environment (VLE) for students and staffs to carry out their academic activities.

- KDU ensures that its eLearning provision can meet the needs of a full range of flexible and independent learning experiences. This includes on and off-campus learners in local and regional settings and covers both blended and fully eLearningcourses.

- KDU ensures that students taking eLearning courses have equity of opportunity asthey are in the university premises are fully aligned to the needs of the e-Learner.

- KDU ensures that eLearning activities have coherence, consistency and transparency the programs are internally coherent and consistent in the way the objectives, content, student activity and assessment, match to each other. It is open and accessible in its design.

- KDU continually works towards ensuring that all systems, both manual and electronic, used in the eLearning context interoperate in the most effective way to provide learners with an effective and increasingly individualized learning environment encompassing all aspects of their experience as a student of the university.

- KDU exploits the range of technologies used in the eLearning context to work withpartner organizations, employers and individuals to assist it in meeting its goals of supporting the independent and lifelong learner and continuing professional development.

- KDU provides Zoom accounts for the lecturers which is provided by the LEARN and the policies related to the zoom accounts are created by the LEARN and KDU is adhering those policies for the zoom accounts as KDU policies for zoom accounts. Any unauthorized or malfunctioned activity related to zoom accounts will be acknowledged according to those policies.

12. Virtual Learning Environment (VLE)

KDU VLE is developed through Moodle Leaning Management System. It is facilitated to each Faculty, Department, Centre to publish their online content and share it with the relevant group of students to access the course contents, materials and do the Assignments. The user accounts of staff and students for the VLE are created by the nominated Faculty admin for each Faculty from the CITS & DS.

a. Creating student accounts and teacher accounts

Faculty coordinator at the respective faculty needs to send a request to Faculty Admin at the CITS & DS by completing the provided template to create student and teacher accounts.

b. Responsibilities of each User Level

i. Faculty Admin (from CITS & DS)

Faculty Admin has been appointed from CITS & DS staff for each Faculty and their responsibilities are

(1) Creating user accounts.

(2) Creating Student groups (Cohorts).

ii. Faculty Coordinator

Coordinate the LMS activities with LMS Admin nominated from CITS & DS Staff and faculty managers, at the respective faculties.

iii. Faculty Manager

Responsible for maintain the privacy of the exams, assignments and continue the Moodle LMS activities, with the help of CITS & DS LMS Admin staff.

(1) New LMS course creation and maintain the exiting courses.

(2) Enroll and un-enroll the students and lecturers to the courses accordingly.

13. LEARN

Lanka Education and Research Network (LEARN) had been in development over 30 years. A National Research and Education Network (NREN) is usually a specialized Internet Service Provider dedicated to supporting the needs of the research and education communities within a country and it is distinguished by support for a high- speed backbone network, often offering dedicated channels for individual research projects. LEARN is an association registered under the Companies Act of Sri Lanka, and works as a specialized internet service provider for education and research purposes. It provides a high-speed backbone network connecting the Ministry of Education, UGC, and state higher education and research institutions. LEARN functioning as an internetservice provider which facilitate university web servers for access to online tertiary education.

14. Role and responsibilities of the students in an eLearning setup

The student is responsible for making their own arrangement for minimum necessary infrastructure support to resolve failures related to facilities.

Students should ensure that they engage with learning materials and mode of delivery. The student should conform to the schedule of the program delivery and assessment, monitor the receipts of materials and alert the relevant lecturer or the coordinator CITS &DS if any material is corrupted or failed to arrive.

15. Use of IT Devices Issued by KDU

IT devices issued by the KDU to a user shall be primarily used for academic, researchand any other university related purposes and in a lawful and ethical way and shall be governed by the practices defined in the Section "Use of IT Devices on KDU Network". The aforesaid section covers best practices related to use of desktop devices, portable devices, external storage media and peripherals devices such as Printers and scanners.

16. Security Incident Management Process

- A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of university's data.
- IA reserves the right to deactivate/remove any device from the network if it is deemed as a threat and can lead to a compromise of a system under intimation to the competent authority of the university.
- Any security incident noticed must immediately be brought to the notice of the IA.

- Notwithstanding anything in the above clause, the disclosure of logs relating to or contained in any IT Resource, to Law Enforcement agencies and other organizations by the IA shall be done as per any applicable laws.
- IA shall neither accept nor act on the request from any other organization, saveas provided in this clause, for scrutiny or release of logs.

17. Intellectual Property

Material and resources accessible through the KDU's network may be subject to the provisions of Intellectual Property Act No.36 of 2003 and protected under privacy, publicity, or other personal rights and intellectual property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information. Users shall not use Material and resources accessible through the KDU's network in any manner that would infringe, dilute, misappropriate, or otherwise violate any suchrights.

18. Enforcement

- This policy is applicable to all the users of KDU as specified in Section 2 of this document. It is mandatory for all users to adhere to the provisions of this policy.
- Each entity of KDU shall be responsible for ensuring compliance with the provisions of this policy. The Implementing Agency (IA) would provide necessary technical assistance to the users who are entities in this regard.

19. Deactivation

- In case of any threat to the security of KDU's systems or network from the resources being used by a user, the resources that are used may be deactivated immediately bythe IA.
- Subsequent to such deactivation, the concerned user and the competent authorityof the university shall be informed.

20. Audit of KDU Network Infrastructure

The security audit of the network infrastructure shall be conducted periodically by an organization approved by the university.

21. IT Hardware Installation

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

- Who is the Primary User?

An individual in whose room the computer is installed and is primarily used by him/her is considered or someone who got the computer legally to do the work in the university from the relevant authority to be the "primary" user. If a computer has multiple users, none of whom are considered the "primary" user, the department Head should make an arrangement and make a person responsible for compliance.

- What are End User Computing Systems?

Apart from the client PCs used by the users, the university will consider servers not directly administered by CITS& DS, as end-user computers. If no primary user can be identified, the respective department/section must assume the responsibilities identified for end-users. Computing systems, if any, that are acting as servers that provide services to other users on the Internet through registered with the CITS& DS and should be under control by the CITS& DS, are still considered under this policy as "end-users" computers.

- Warranty & Annual Maintenance Contract

Computers purchased by any Section/ Department/ Project should preferably be with 3 years onsite comprehensive warranty. Such maintenance should include standard repair and maintenance procedures as may be defined by CITS&DSfrom time to time.

- Power Connection to Computers and Peripherals

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

- Network Connection

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

- File and Print Sharing Facilities

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

- Maintenance of Computer Systems provided by the University

Computers to be purchased not centrally, but the specific requirement and purchase of the respective Faculties/ Departments/ Sections. CITS & DS will attend to the complaints related to any maintenance-related problems.

22. Software Installation and Licensing

Any computer purchases made by the individual departments/projects should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed. In compliance with the Computer Crimes Act No.24 of 2007 and Intellectual Property Act No. 36 of 2003, the university IT policy does not allow any pirated/unauthorized software installation on the university-owned computers and the computers connected to the university campus network. In case of any such instances, the university will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

- Operating System and its Updating

Individual users should make sure that respective computer systems have their OS updated in respect of their service packs/patches, through the internet. Checking for updates and updating the OS should be performed at least once a week or so. As a policy university encourages the user community to go for open-source software such as Linux, Open Office (Open-Source Operating Systems) to be used on their systems wherever possible.

- Use of software on Desktop systems

1. Users shall not copy or install any software on their own on their desktop systems, including privately owned shareware and freeware without the approval of the respective authority.

2. Any software installed should be for activities of the university only.

- Antivirus Software and its updating

Computer systems used in the university should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy.

Individual users should make sure that respective computer systems have current virus protection software installed and maintained. If not, they have to inform CITS & DS at the first instance of noticing.

- Backups of Data

Individual users should perform regular backups of their vital data. Users should keep their valuable data backups in external storage devices such as pen drives, external HDD etc. CITS & DS has to take action to establish the DR Site and arrange for the backup system for centrally handled data.

23. Use of IT Devices on KDU Network

This section provides the best practices related to the use of desktop devices, portable devices, external storage media and peripheral devices such as printers and scanners on KDU's network.

25.1 Desktop Devices

1. Use and Ownership

   Desktops shall normally be used only for transacting university's works. Users shall exercise their own good judgment and discretion towards the use of desktop devices for personal use to the minimum extent possible.

2. Security and Proprietary Information

   a. The user shall take prior approval from the IA to connect any access device tothe KDU's network.
   b. User shall keep their passwords secure and not share their account details. Users shall keep strong and secure passwords as per the

password policyof the application.

c. All active desktop computers shall be secured with a password-protectedscreensaver which should be set with automatic activation at 10 minutesor less, or log-off when the system is unattended.

d. Users shall ensure that updated virus-scanning software is running in all systems. Users shall exercise due caution when opening e-mail attachments received from unknown senders as they may contain viruses, e-mail bombs, or Trojan horse code.

e. The user shall report any loss of data or accessories to the competent authority of KDU.

f. The user shall obtain authorization from the competent authority before taking any KDU-issued desktop/Laptop outside the premises of the university.

g. Users shall properly shut down the systems before leaving the office/ department.

h. Users shall abide by instructions or procedures as directed by the CITS &DS from time to time.

i. If users suspect that their computing system has been infected with a virus (e.g. it might have become erratic or slow in response), it should be reported to the IA (CITS & DS) for corrective action.

25.2 Sharing of data

Users shall not share their account(s), passwords, Personal Identification Numbers (PIN), digital signatures certificate or similar information or devices which is used for identification and authorization purposes.

25.3 Use of Portable devices

Devices covered under this section include KDU-issued laptops, mobiles, iPads, tablets, PDAs etc. Use of the devices shall be governed by the following:

a. User shall be held responsible for any unauthorized usage of their KDU-issued access device by a third party.

b. Users shall keep the KDU-issued devices with them at all times or

store them in a secured location when not in use. User should not leave the devices unattended in public locations (e.g. classrooms, meeting rooms, restaurants etc.).

c. User shall ensure that the portable devices are password protected and auto lockout enabled. The password used should be as strong as the device may support and should be as per the password policy of the application.

d. CITS & DS shall ensure that the latest operating system, anti-virus and application patches are available on all the devices, in coordination with the User. Firewalls shall be enabled, if possible.

e. Users shall wipe or securely delete data from the device before returning/ disposing it off.

f. Lost, stolen, or misplaced devices shall be immediately reported to the IA.

g. When installing software, user shall review the application permissions to ensure that unwanted information regarding the user is not shared with the application provider.

24. Network Use

Network connectivity provided through the university, referred to hereafter as "the Network", either through an authenticated network access connection or a Virtual Private Network (VPN) connection, is governed under the university IT Policy. The CITS &DS is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the university's network should be reported to CITS &DS.

- IP Address Allocation

Any computer (PC/Server) that will be connected to the university network, should have an IP address assigned by the CITS &DS. Following a systematic approach, the range of IP addresses that will be allocated will be based on Virtual LAN (VLAN) created against each entity or objective. Any device connected to the network will be allocated an IP address only from that address pool. Further, each network port in the room from where that computer will be connected will have binding internally with that IP address so that

no other person uses that IP address unauthorized from anyother location. As and when a new computer is installed in any location, it will be allocated as per the DHCP pool policies.

An IP address allocated for a particular computer system should not be used on any other computer even if that other computer belongs to the same individual and will be connected to the same port. The IP address for each computer should be obtained separately by filling up a requisition form meant for this purpose.

- DHCP and Proxy Configuration by Individual Departments /Sections/ Users

  Use of any computer at the end user location as a DHCP server to connect to morecomputers through an individual switch/hub and distributing IP addresses (publicor private) should strictly be avoided, as it is considered an absolute violation of the IPaddress allocation policy of the university. Similarly, a configuration of proxy serversshould also be avoided, as it may interfere with the services run by the CITS &DS.

Even configuration of any computer with an additional network interface card and connecting another computer to it is considered a proxy/DHCP configuration. Non-compliance with the IP address allocation policy will result in disconnecting the port from which such a computer is connected to the network. The connection will be restored after receiving written assurance of compliance from the concerned department/user.

- Running Network Services on the Servers

a. Departments/individuals connecting to the university network over the LAN may run server software, e.g., HTTP/Web server, SMTP server, FTPserver, only after bringing it to the knowledge of the CITS &DS in writing and after meeting the requirements of the university IT policy for running such services. Non-compliance with this policy is a direct violation of the university IT policy, and will result in the termination of their connection tothe Network.

b. CITS &DS takes no responsibility for the content of machines connected to the Network, regardless of whether those machines are university or personal property.
c. CITS &DS will be constrained to disconnect client machines where potentially damaging software is found to exist. A client machine may also be disconnected if the client's activity adversely affects the Network's performance.
d. Access to remote networks using a university's network connection must be in compliance with all policies and rules of those networks. This applies to any networks to which the university Network connects. university network and computer resources are not to be used for personal commercial purposes.
e. Network traffic will be monitored for security and for performance reasons at CITS &DS.
f. Impersonation of an authorized user while connecting to the Network is in direct violation of this policy and will result in the termination of the connection.

- Internet Bandwidth obtained by Other Departments

a. Internet bandwidth acquired by any department of the university under any research program/project should ideally be pooled with the university's Internet bandwidth, and be treated as the university's common resource.
b. Under particular circumstances, which prevent any such pooling with the university Internet bandwidth, such a network should be totally separated from the university's campus network. All the computer systems using that network should have separate VLANs based on grouping criteria.
c. IP address scheme (private as well as public) and the university gateway should not be specified as an alternative gateway. Such networks should be adequately equipped with necessary network

security measures as laid down by the university IT policy. One copy of the network diagram giving the details of the network design and the IP address schemes usedmay be submitted to CITS &DS.

d. Non-compliance with this policy will be a direct violation of the university's IT security policy.

25. E-mail Account Usage

KDU provides official email access privileges to its users. In an effort to handle the efficient information dissemination among the administration, faculty members, staff and students, it is recommended to avail official e-mail with KDU's domain.

In an effort to increase the efficient distribution of critical information to all faculty,staff and students, and the university's administrators, it is recommended to utilize the university's e-mail services, for formal university communication and for academic & other official purposes.

E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal university communications are official notices from the university to faculty, staff and students. These communications may include administrative content, such as human resources information, policy messages, general university messages, official announcements, etc.

To receive these notices, it is essential that the e-mail address be kept active by using it regularly. Staff and faculty may use the e-mail facility by logging on to http://office.com with their User ID and password. For obtaining the university's e-e-mail account, a user may contact CITS &DS for an e-mail account and default password by submitting a request through the department/section authorities.

Users may be aware that by using the e-mail facility, the users are agreeing to abide by the following policies:

- The facility should be used primarily for academic and official purposes and to alimited extent for personal purposes.
- Using the facility for illegal/commercial purposes is a direct violation of the university's IT policy and may entail withdrawal of the facility. The illegal

use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages. And generation of threatening, harassing, abusive, obscene or fraudulent messages/images.

- While sending large attachments to others, user should make sure that the recipient has e-mail facility that allows him to receive such large attachments.
- Users should keep the mailbox used space within about 80% usage threshold, as 'mailbox full' or 'mailbox almost full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
- Users should not open any mail or attachment that is from an unknown and suspicious source. Even if it is from a known source, and if it contains any attachment that is suspicious in nature or looks dubious, a user should get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of security of the user's computer, as such messages may contain viruses that have the potential to damage the valuable information on your computer and the Network.
- Users should not share his/her e-mail account credentials with others, as the individual account holder is personally held accountable, in case of any misuse of that e-mail account.
- Users should refrain from intercepting or trying to break into others e-mail accounts, as it is infringing the privacy of other users.
- While using the computers that are shared by other users as well, any e-mail account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.
- Impersonating the e-mail accounts of others will be taken as a serious offence under the IT security policy.
- It is ultimately each individual's responsibility to keep their e-mail account free from violations of university's e-mail usage policy.

- All the mails detected as spam mails go into the SPAM_MAIL folder of the respective users' mail accounts. Users are requested to open these folders periodically to check any important mail wrongly stamped as SPAM mail and went into this folder. It is recommended to empty this folder as frequently as possible.

- E-mail Password standard;

Minimum Length	Combination	Change Frequency	Reset Mechanism
8	At least 1 uppercase(A-Z) and one lowercase(a-	Annually	Self-service reset if valid mobile and secondary e- mail are set up at the time of registering.
	z) character, 1 number (0-9), and 1 special symbol (Ex: @ #)		Or on Email Request to Director CITS & DS

The above laid down policies particularly 1 to 11 are broadly applicable even to the e-mail services that are provided by other service providers such as Gmail, Hotmail, Yahoo, etc., as long as they are being used from the university's campus network, or by using the resources provided by the university to the individual for official use even from outside.

26. Disposal of ICT equipment

The disposal of ICT hardware equipment shall be done as per the Standard Operating Procedures of the E-Waste Management of the country.

27. Breach of This Policy

Users are encouraged to be vigilant and to report any suspected violations of this Policy immediately to the Director IT (directorit@kdu.ac.lk). On receipt of notice (orwhere

the university otherwise becomes aware) of any suspected breach of this Policy, the university reserves the right to suspend a user's access to university's Data.

If any breach of this Policy is observed, then (in addition to the above) disciplinary action up to and including dismissal in the case of Staff, expulsion in the case of Students or contract termination in the case of third parties may be taken in accordance with the university's disciplinary procedures.

6. Definitions

(a)

(b)

(c)

7. Responsibility

The following roles and responsibilities are envisaged from each entity respectively;

1. CITS & DS shall ensure the resolution of all incidents related to the security aspects of this policy by their users. They shall provide the requisite support in this regard.
2. Use KDU's IT resources for those activities that are consistent with the academic, research and public service mission of the university and are not "Prohibited Activities".
3. All users shall comply with existing national, state, and other applicable laws.
4. Abide by existing Telecommunications and Networking laws and regulations.
5. Follow copyright laws regarding protected commercial software or intellectualproperty.
6. As a member of the university community, KDU provides use of scholar and/or work-related tools, including access to the library, certain computer systems and servers, software and databases and the Internet. It is expected from university Community to have a reasonable expectation of unobstructed use of these tools, of certain degrees of privacy and of protection from abuse and intrusion by others sharing these resources. Authorized users can expect their

right to access information and to express their opinion to be protected as it is for paper and other forms of non- electronic communication.

7. Users of KDU shall not install any network/security device on the network without consultation with the Implementing Agency (CITS & DS).
8. It is a responsibility of the university Community to know the regulations and policies of the university that apply to appropriate use of the university's technologies and resources. University Community is responsible for exercising good judgment in the use of the university's technological and information resources. Just because an action is technically possible does not mean that it isappropriate to perform that action.
9. As a representative of the KDU community, each individual is expected to respect and uphold the university's good name and reputation in any activities related to use of ICT communications within and outside the university.

8. Implementation

1. KDU shall implement appropriate controls to ensure compliance with this policy by their users. Center for IT Support & Development Services (CITS & DS) shall be the primary Implementing Agency (IA) and shall provide necessary support for the implementation of the policy.

2. Implementing Agency of KDU should ensure proper dissemination of this policy.

9. Policy Review and Amendments

a) This policy may have reviewed after every three years or earlier as necessary.

b) Sub revisions may be initiated on the recommendation of the Director IT and/or the directions of the Vice- Chancellor of KDU

c) Any such revision and/or amendments shall be forwarded for the recommendation of the Senate, and become effective from the approved by the BoM of the University.