COLLEGE OF BUSINESS EDUCATION

PROPOSED INFORMATION AND COMMUNICATION TECHNOLOGY GUIDELINES

June, 2018

FOREWORD

The College of Business Education depends heavily on ICT to carry out its day to day business operations. In many ways ICT has helped the College to improve its operations and delivery of services. This include students' admission and registration, academic and finance operations. The maximum dependence on ICT has triggered a need for an ICT Policy and ICT guidelines. Development and implementation of these guidelines will enable efficient and timely delivery of services.

By recognizing the impact of ICT in achieving CBE's objectives, the College has deployed several ICT systems for effective and efficient service delivery. Some of these systems can only be accessed internally while others outside the College. The College further understands that ICT systems are vulnerable to attacks and there are threats which need mechanisms to protect organizational ICT resources against threats and attacks. In addition, improper handling of organizational data would infringe rules and regulations governing data confidentiality, integrity and availability. Moreover, the College has computer department to oversee proper utilization of ICT resources as well as monitor all ICT activities while ensuring that they are conducted according to the best practices.

Thus, the ICT guidelines provide mechanisms for guiding both, the handling and use of ICT facilities of the College. The Guidelines put forward best practice when using College ICT facilities. These Guidelines are in line with the National ICT Policy 2016, CBE ICT Policy 2017, and other relevant College policies that aim at creating a proper handling and use of ICT facilities.

A number of stakeholders have been involved in the development of this document. While it is not possible to mention everyone's name, however, we acknowledgment their great contributions in putting these CBE ICT guidelines in place.
It should be clear that, in a scenario where an ICT facility user fails to comply with these guidelines; Disciplinary measures will be taken against them as per Public Service Acts, Regulations, Circulars and other College rules and procedures. It is therefore my expectation that all users will adhere to these guidelines set here forthwith.

Prof. Emanuel Mjema
RECTOR

COLLEGE OF BUSINESS EDUCATION INFORMATION COMMUNICATION TECHNOLOGY GUIDELINES

PART I

PRELIMINARY PROVISIONS

Citation

1. This guideline must be cited as College of Business Education Information Communication Technology guideline.

Application

2. This guideline shall apply to all CBE ICT resources' users

Interpretation

3. In this guideline unless the context otherwise requires-

"Access" in relation to any ICT system, means entry to, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of the computer system or network or data storage medium;

"**Bandwidth**" means amount of data a network can transmit in a certain period of time usually expressed in megabytes per second (Mbps);

"Computer system" means a device or combination of devices, including network, input and output devices capable of being used in conjunction with external files which contain computer programs, electronic instructions, input data and output data that perform logic, arithmetic data storage and retrieval communication control and other functions;

"Computer data" means any representation of facts, concepts, information or instructions, in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

"**Cloud computing**" means the delivery of ICT services as a service on computing resources such as applications, software, infrastructure as well as platforms over the Internet without necessarily hosting servers at CBE;

"**Data backup**" means a system of recording identified data onto portable media.

"**Data storage medium**" means any device, article or material from which computer data or information is capable of being stored or reproduced, with or without the aid of any other device or material;

"Device" means electronic equipment which can include: -

a) a computer program, code, software or application;
b) component of computer system such as graphic card, memory card, chip or processor;
c) computer storage component;
d) input and output devices;

"Document" means any recorded information or material, in electronic format or print, which conveys coherent information for human understanding and use.

"**E-resources**" means Information resources that user accesses electronically including, but not limited to electronic journals, electronic books and other web-based documents;

"**Free Open Source Software**" means computer software that anyone is freely licensed to use, copy, study, and modify the software in any way, and the source code is openly shared so that people can modify or improve the design and its performance;

"**E-waste**" means non-usable desktop computers, notebook or laptop computers, CD-ROM and DVD equipment, data projectors, digital cameras, telephones, mobile phones and personal digital assistants (PDAs), printers, photocopiers, fax machines and multifunction devices (MFDs), keyboards and similar peripheral ICT devices, servers, hubs, switches, bridges, routers, power supplies and batteries, UPS, scanners, electronic entertainment devices and consoles, and other

similar items. This definition includes used electronic equipment destined for reuse, resale, salvage, recycling, or disposal;

"hyperlink" means a symbol, word, phrase, sentence or image that contains path to another source that points to and causes to display another document when executed;

"**Information and Communication Technologies (ICT)**" means a diverse set of tools, systems, applications and services used for production, processing, storage, transmission, presentation and retrieval of information by electronic means;

"**Information Systems Audit"** means an examination of the controls within an entity's Information technology infrastructure. These reviews may be performed in conjunction with a financial statement audit, internal audit, or other form of attestation;

"intellectual property rights" means the rights accrued or related to copyright, patent, trademark and any other related matters;

"**Institutional repository**" means online database for collecting, preserving, and disseminating the intellectual output of an institution. The collection includes but not limited to materials such as journal articles particularly preprints, theses and dissertations, research reports, course notes, and other academic documents;

"**Internet**" means a collection of private and public router-based networks that are interconnected via gateways and exchange points, which all utilize the TCP/IP protocol.

"Internet Protocol Address (or IP Address)" means a unique address that computing devices use to identify itself

and communicate with other devices in the Internet Protocol network;

"**Local Area Network (LAN)**" means computer network that spans a relatively small area such as a single building or group of buildings;

"**Management Information Systems**" means information systems used as tools to facilitate the management of corporate functions;

"**ICT Equipment**" means any electronic device used for Information and Communication Technologies including desktop computers, laptops, servers, monitors, printers, audio-visual(AV) equipment, software and network equipment;

"ICT facility" means a place or piece of equipment that uses information and communication technology including physical devices, internet facilities - both wireless and wired;

"Modular object-oriented dynamic learning (Moodle)" means open source learning platform designed to provide educators, administrators and learners with a single robust, secure and integrated system to create personalized learning environments. This also can refer to Modular Object-Oriented dynamic learning environment.

"**Parallel Running**" means a process of running a new or amended system simultaneously with the old system to confirm that it is functioning properly before complete migration;

" **Publish**" means distributing, transmitting, disseminating, circulating, delivering, exhibiting, exchanging, printing, copying, selling or offering for sale, letting on hire or offering to let on hire, offering in any other way, or making available in any way;

"**Physical access**" means the ability of a person to gain access to physical facilities (e.g., buildings, computer, server rooms, warehouses);

"Remote site" means a site which is away from the main server which includes but not limited to campuses, colleges, and hostels;

"Restricted system" means system which does not allow unauthorized users to access;

"**Rootkits**" means a type of Trojan that keeps itself, other files, registry keys and network connections hidden from detection;

"**Software Change Management**" means a process of planning, organizing, controlling, executing and monitoring changes that affect the delivery of ICT services;

"**System Administrator**" means person who supports multi-user computing environment and ensures continuous, optimal performance of IT services and support systems;

"Spam" means unsolicited messages sent typically to large numbers of users, for the purposes of advertising, phishing, spreading malware;

"**Structured Cabling**" means a set of cabling and connectivity products that integrates voice, data, video, and various management systems of a building (such as safety alarms, security access, energy systems, networks etc.);

Transmission Control Protocol/Internet Protocol (TCP/IP) is a basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet)

"**Trojan**" means a program that appears legitimate but performs some illicit activity when run; It may be used to locate password information or make the system more vulnerable to future entry or simply destroy the user's stored software and data, Trojan is similar to a virus, except that it does not replicate itself;

"**Trusted Cloud Computing Vendor**" means person or company that has high level of confidentiality, uses server, and client authentication, security domains, cryptograph in data separation, and certificate-based authorization;

"**Computer Department**" means the College unit dealing with ICT matters in delivering services;

"**College**" means College of Business Education (CBE);

Uninterruptable power supply (UPS) is an electrical apparatus that provides emergency power to a load when the input power source, typically mains power fails.

"Unsolicited messages" means communication that:

(1) does not have one of the following qualities

(a) the receiver does not consent to such communication and has evidently shown to the sender,

(b) at the beginning of the communication, the communication does not disclose the identity of sender and its purpose; and

(c) That communication does not give an opt-out option to reject further communication.

(2) The consent requirement is deemed to have been met where-

(a) the contact of the addressee and other personal information were collected by the originator of the message in the course of work or business relations;

(b) the originator only sends promotional messages relating to its similar products and services to the addressee;

(c) the originator offered the addressee the opportunity to opt-

out and the addressee declined to opt-out; and

(d) an opportunity to opt-out is provided by the originator to the addressee with every subsequent message.

"**User"** means any person authorized to use College ICT facilities;

"**Virus**" means a software used to infect a computer after the virus code is written; it is buried within an existing program and once that program is executed, the virus code is activated and attaches copies of itself to other programs in the computer and other computers in the network;

"**Wide Area Network (WAN)**" means a geographically dispersed telecommunications network, thus computers connected to a *wide-area network* are often connected through public *networks*, such as the telephone system. They can also be connected through leased lines or satellites; and

"**Wireless Network**" means network that does not require cable connections.

Disclaimer

4. The College undertakes to provide and operate its ICT resources with reasonable skill. However, the College accepts no liability for any loss or damage a user may suffer from any failure or malfunction of the College ICT resources or any part thereof.

PART II

GENERAL GUIDELINES

Purpose of Guidelines

5. The main purpose of this guideline is to provide framework for governance which includes selecting, implementing, and managing Information and Communication Technology (ICT) services by guiding the College on how to manage ICT facilities.

ICT facility Procurement and Installation

6. In order to best utilize funds generated by CBE or from donors for acquisition of ICT facilities or resources the following issues are to be taken into consideration: -
   (i) Compatibility across College computers, network and software systems.
   (ii) Lowest cost and most reliability for operation, warranty work and maintenance on the software and hardware acquired.
   (iii) Lowest life – cycle cost for the College ICT equipment as a whole.

7. On acquiring hardware and software, proper procurement procedures shall be followed as stated in the Public Procurement Act and its Regulations.

8. ICT facilities or resources that meet the College standards can be purchased from vendors within the country or ordered directly from abroad if necessary. Specifications for computers and related equipment to be purchased will be provided by Computer Department or in special cases by consultant.

9. Acquisition of all ICT facilities or resources shall be done upon approval of specifications by the College Computer department.

10. ICT hardware and software shall be supplied by a supplier with the relevant manufacturers' authorization.

11. All ICT hardware using power shall always be supported by an un-interruptible power supply/surge protector for protection from power surges.

12. ICT hardware shall have a valid warranty of not less than one year.

13. CBE Computer department shall comply with national and international standards to ensure that no inferior ICT equipment/ facilities are supplied to the College.

14. All LAN switches, routers, and firewalls connecting College network segments can be both manageable and unmanageable depending on the situation.

15. Prior recommendations from the College Computer department, all Ethernet switches, routers, and firewalls shall support a minimum transmission and uplink speeds to clients, as well as local server and backbone connectivity.

16. Installations and configurations of acquired ICT facilities or resources will be performed by computer department personnel, and by suppliers for those ICT facilities or resources which requires special expertise. If installation and configuration of any ICT facilities or resources is to be done by outsider (supplier) computer department personnel will be involved.

Software management

17. To ensure effectiveness, high performance, and higher security, College computers and related devices shall be supplied with free and open source (FOS) Operating System (OS) whenever possible.

18. Without prejudice to guideline 17; in case a computer requires a proprietary (commercial) OS, it must be supplied with genuine and licensed OS which is recommended by experts from the Computer department.

19. Software shall be developed by CBE, for those which will be acquired from software suppliers and implemented at the College, acquired package must fit CBE requirements.

20. For software acquired from suppliers there should be agreements between CBE and the software suppliers. The agreements should state the license issues, supporting and training issues if any. In some cases, acquisition of software includes training and special offers for academic institution like CBE, in this case the benefits should also be stated in the agreement.

21. All information systems that support teaching, research, service delivery and records management application software installed in College computers must be approved by College Computer department.

22. All computers with OS susceptible to viruses attack must be installed with genuine, licensed and up-to-date anti-virus.

23. All software customization shall comply with College requirements and CBE ICT security guidelines.

24. Designated officer shall verify that need for a particular customization has been met.

LAN Cabling

25. In case where cabling system provides telecommunication services from Floor Distribution to the Telecommunication Outlet(s), copper cabling shall be used. However, where necessary fiber optic or any other acceptable cabling standards such as EGA, ISO, ISEC may also be used.

26. In case the cabling system provides data and/or telecommunication services between buildings such that it connects two or more Building Distribution(s); it must be in the form of fiber optic cabling. However, for remote sites, a

suitable wireless technology may be required.

ICT Equipment Rooms

27. Anyone responsible for the specification of the equipment rooms should seek advice from the relevant College Computer department.

28. Water/steam pipes shall never be installed directly above or in the same room as telecommunications equipment.

29. When planning the location, size and number of equipment rooms required anyone responsible for the design and planning of the computer network cabling infrastructure shall keep in mind the 90-meter rule for the Horizontal Cabling Subsystem.

30. All ICT equipment rooms shall house only equipment directly related to the Structured Cabling infrastructure, associated electronics and its environmental support systems including suitable earth connection.

31. Equipment and services not directly related to the support of the Server/Computer and Telecommunications rooms or Structured Wiring System shall not be installed in, pass through, or enter the aforementioned rooms.

32. During the structured cabling installation project the project manager must present a Telecommunications Room layout to the relevant authority.

Communication Cabinets (Racks)

33. The location of the Communications Cabinets must provide physical and environmental protection for the telecommunications equipment against temperature, humidity, vibration, extortion, posture to ultraviolet radiation, ingress of dust, fluids or other contaminants, physical damage (accidental or malicious), security, electromagnetic interference and other hazards.

34. Communication Cabinets should allow adequate access and

should be provided with illumination and temperature conditions suitable to allow installation and maintenance of a Structured Cabling System and associated electronics.

35. Communications Cabinets shall be located such that subsequent measurements, repair, expansion or extension of the installed cabling can be undertaken in safety.

36. During the structured cabling installation project the Network Installation Project Manager must issue a Cabinet layout detailing subsystem terminations, equipment locations and associated devices.

37. Terminals, wires, ports shall be labeled for easy maintenance

Servers and Server Room Security

ICT Security

38. Server rooms shall be non-smoking zones, fitted with smoke detectors and have automatic or portable fire extinguisher systems.

39. All server rooms shall be protected against unauthorized access. The authorization of access to Server Rooms and Disaster Recovery Site shall be based on the following requirements:
    a. Staff/Visitors permitted to enter the Server rooms must be accompanied by designated officer. Visitors shall be logged in the register book.
    b. Access to the server room shall be restricted by key, code, or electronic card. The process for issuing keys, codes, and/or cards must be documented.

40. Identification cards shall not be shared or exchanged.

41. Access to the ICT systems shall be authorized by the relevant authority, or appropriate delegated officer.

42. Access to any particular data file should be based on the user's roles as established by his or her official duties, and

should be reflected in the provision of specific authorization codes, passwords or other access-enabling means.

43. User shall be issued with Unique User Identities (IDs) that are produced following a standard naming convention. The naming conversation shall identify at least two names of the user. e.g. first name.lastname

44. Before being granted logical access, user shall complete a "User Access Permission Application Form" that defines access privileges and roles.

45. Changes to access roles and privileges should only be made under authorization of the relevant authority.

46. Designated Systems administrators shall review and maintain User Access Profiles.

47. Privileges shall be allocated to network and/or application software accounts on an 'as needs' basis.

48. For security reasons, user account names shall not indicate users associated privileges.

49. All changes to network configurations shall be recorded in the register, along with authorization for the changes.

50. User shall be permitted to use only those network addresses issued to them by the relevant authority.

51. Remote user shall connect to servers using a secure communication channel such as Virtual Private Network or SSH on dedicated communication lines with end-to-end encryption.

52. Results/Logs from the firewall shall be reviewed by system administrator to confirm there have been no unexpected attempts to connect.

53. Login to systems using system super user is strictly prohibited unless the system administrator has no other means to change configurations.

54. Passwords must be changed frequently at a maximum of one-month interval.

55. Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:

    a. Server contact(s) and location, and a backup contact

    b. Hardware and Operating System/Version

    c. Main functions and applications, if applicable

    d. Information in the corporate enterprise management system must be kept up-to-date.

    e. Configuration changes for application servers must follow the appropriate change management procedures.

General Configuration Guidelines

56. Services and applications that will not be used must be disabled where practical.

57. The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

58. Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.

59. Always use standard security principles of least required access to perform a function.

60. Do not use root when a non-privileged account will do.

61. If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).

Security of Media in Transit

62. Information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance when sending media via the postal service or via courier. Thus, it is important to safeguard computer media being transported between sites based on the following principles;
    a. Reliable and trusted transport or couriers should be used.
    b. Packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with manufacturers' specifications.
    c. Special controls should be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification e.g. by use of locked containers, delivery by hand, or use of tamper-evident packaging.

Security of Equipment rooms

63. Access to the equipment rooms must be restricted to authorized personnel only, as specified by the College Computer department, thus maintaining a degree of security and minimizing the risk of damage which could threaten the integrity of the network.

64. All doors that have direct access to equipment rooms shall be fitted with swipe card access or have security lock.

65. All windows within the equipment rooms must be fitted with opaque glass. Iron bars must be fitted to the inside of the windows.

Internet use

66. CBE shall strike a balance between taking advantage of the Internet and maintaining security and confidentiality based on the following principles:
    a. The prudent bandwidth management practices shall be observed to assign highest priority to mission critical traffic (critical traffic to maintain the College's Internet presence). This includes traffic to and from student records information system, e-Learning system, College maintained web and email servers. Mission critical traffic also includes traffic to and from Library databases and systems, hosted resources critical to finance and human resource.
    b. Peer-to-peer file sharing, Non-academic traffic, video streaming, large file transfers and system updates shall be given less priority; however, a dedicated bandwidth will be allocated for video conferencing.
67. System administrators shall monitor network traffics and generate appropriate reports for decision making.

68. For all traffic the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic. Internet Use records must be preserved for at least 3 months.

69. System administrators shall follow all best practices provided by the College Computer department.

70. The College shall ensure that there is control of spam by using e-mail filtering tools in e-mail software to block or screen out spam by defining some simple filtering rules.

71. The College shall strive to ensure that network is protected from malware and/or hackers that come with the use of Internet.

72. Internet service/connection shall not be used to perform illegal acts and unauthorized activities.

73. All access to the Internet shall be routed through firewalls and monitoring software.

74. The designated network administrator shall ensure that the security of information in LAN and protection of supporting infrastructure are based on the following requirements;

75. LAN shall not be extended to other remote networks without permission of the Computer department;

76. System administrators shall ensure that unauthorized traffic will not be allowed to enter the College LAN

77. System Administrator shall encrypt data with approved encryption algorithm before transmitting over the network.

78. The College shall ensure that firewalls, intrusion prevention and detection system shall be installed and properly configured to protect LAN.

79. The College shall ensure that, all access points of the LAN layout are identified, and checks to verify that safeguards are operational.

Internet Use Filtering System

80. System administrators shall block access to Internet websites and protocols that are deemed inappropriate for CBE's corporate environment. The following protocols and categories of websites should be blocked:
    a. Adult/Sexually Explicit Material
    b. Gambling
    c. Hacking
    d. Illegal Drugs
    e. Peer to Peer File Sharing

f. Personals and Dating
g. SPAM, Phishing and Fraud
h. Spyware
i. Tasteless and Offensive Content
j. Violence, Intolerance and Hate

Internet Use Filtering Rule Changes

81. Information Systems and Library Services Committee (ISLC) shall periodically review and recommend changes to web and protocol filtering rules. Changes to web and protocol filtering rules will be recorded in this guidelines document.

82. Employees may access blocked sites with permission if appropriate and necessary for business purposes. If an employee needs access to a site that is blocked and appropriately categorized, they must submit a request to computer department by email. Once the request is approved computer department will unblock that site or category. System administrator will track approved exceptions and report on them upon request.

83. Security controls shall be based on following principles:
    a. System administrators shall ensure that all changes in the systems are documented and such documentation is physically secured. The documentation shall be inspected by the head of the College Computer department from time to time.
    b. Wireless network shall be used with sufficient authentication and transmission encryption measures in place, complemented by proper security management processes and practices.
    c. System Administrators shall develop a coverage map of the wireless network, including locations of respective access points and Service Set Identifier (SSID) information so as to avoid excessive coverage by the wireless signal.
    d. System Administrators shall regularly search for rogue or unauthorized wireless access points.
    e. Once a device is no longer connected to the College

network, System Administrators shall modify the encryption keys and SSID

f. The System Administrators shall change product default access point configuration settings.
g. The System Administrators shall disable all insecure and unused management protocols on access points.
h. The System Administrators shall enable and configure security settings to make sure that unauthorized users do not gain access to wireless network.
i. The System Administrators shall ensure all wireless connections are connected to the security equipment (e.g. firewall, router).
j. The System Administrators shall activate logging features and redirect all log entries to a logging server. The log records should be checked regularly.
k. The System Administrators shall keep strict control of the wireless interface cards (e.g. PCMCIA card for laptop) as access credentials such as SSID and/or encryption key are commonly stored on the card.
l. The System Administrators shall give guideline protection against computer virus and malicious code to users.
m. Appropriate locks on windows and doors should be maintained.
n. Doors shall be kept locked when rooms are not in use.
o. Secure system for keys and combinations should be maintained.
p. In the event of security breach, compromised lock should be changed and alternative physical security strategies should be used when appropriate.
q. All legitimate visitors should be logged at the entrance to CBE building and must declare ICT equipment.
r. All staff must declare personal ICT equipment at the entrance in server and computers rooms

ICT Change Management

84. All stakeholders shall be responsible to integrate ICTs in their activities to embrace e-governance practices.
85. Change management approach shall be employed to ensure

thoughtful planning and implementation of ICT issues with involvement of stakeholders affected by respective ICT changes.

86. Whenever necessary, user shall be consulted from time to time to support and facilitate the effective implementation of the ICT policy.

87. The College shall ensure that;
    a. A comprehensive change management procedure is documented to all stages of the change management process. The procedure shall contain information regarding the process and responsibilities for change identification, the approval process and the emergency change process.
    b. A formal review before the change is closed on the system.
    c. User requirement analysis is performed prior to the development of /or procurement of the systems or software.
    d. Compatibility of a systems and software are formally documented for better management of the change process.
    e. System checking is performed prior to the change being marked as complete.
    f. Documented evidence of testing retained for future reference.
    g. Inventory updated in the event of change.

System integration and interoperability

88. In order to ensure convenience, efficiency, consistency and accuracy integrity and availability of data and information, all CBE information systems should be integrated.

89. Any new system shall be compatible and interoperable with existing system without compromising organizational security.

90. Different existing systems shall be integrated by adhering to ICT security standards.

91. The Computer department shall be responsible to ensure the guidelines for systems integration and interoperability are adhered to.

Upgrades and contingency plans

92. Installation of new software or upgrade or any hardware should be done by suitably qualified, trained or under supervision of personnel from Computer department.

93. A suitable contingency plan shall be in place in case of failure of the new software or hardware.

94. System Administrator shall properly test new or upgraded software or hardware before using in a live environment based on approved pre-designed test plan.

95. Upgraded software versions shall offer at least the current level of security safeguards.

96. System Administrator shall decide the specific criteria and cut-off date, which will trigger a reversion.

97. System Administrator shall always ensure that an upgraded software version can read and write files in the older format.

98. College Computer department shall strive to ensure that major upgrades of operating system version on servers are done without interrupting the client services.

Applying patches/service packs

99. If patches are applied incorrectly or without adequate testing, the system and its associated information can be placed at risk, possibly corrupting data files. Patches applied to resolve software bugs shall only be applied when verified as necessary and with authorization from the Computer department based on the following requirements:
    a. Patches should be from a reliable source and are to be thoroughly tested by the system administrator before use.
    b. System administrator shall verify that the patches are

necessary and came from an authorized source, normally the software manufacturer or vendors.

c. System administrator shall ensure that updates to the system documentation are received with the patches.

Parallel Running

100. ICT facility testing shall incorporate a period of parallel running prior to the new or upgraded software being acceptable for use in the live environment.

101. A parallel run phase shall be incorporated in the User Acceptance Test Plan.

102. System Administrator shall ensure that the systems are mirrored.

103. In a scenario where two systems are running parallel and that the old one is intended for phasing out, the maximum time for parallel running may not exceed twelve months.

104. Where results differ significantly between the old and new system, the old system may continue to be used until the new system is up and running or otherwise agreed as acceptable.

105. On occasion, changes of an "emergency" or critical nature may be required to quickly address production issues arising in case of emergency. Changes shall be rectified urgently while still maintaining the proper levels of approval, logging, monitoring, communication and closure of all change related activities.

E-Waste Management

106. CBE shall ensure that

a. Only designated collection and disposal points will be used for e-Waste.

b. Equipment shall be disposed if it is free from sensitive or confidential information.

c. E-Waste equipment shall be disposed-off or recycled in an environmentally and socially friendly manner in

accordance with the National Environmental Act.

d. No electronic equipment and e-Waste will be placed in general refuse bins.

107. The coordination of activities associated with the appropriate handling and disposal of e-Waste shall be the responsibility of the CBE Procurement Management Unit (PMU) in abidance with National Environmental Management Council (NEMC) and environmental experts within CBE.

108. During disposal, records shall be maintained to document the amount of e–Waste disposed-of each year in accordance with reporting requirements demonstrating compliance with environmentally friendly initiatives.

Precautions against fire

109. Smoke detectors and fire extinguishers should be regularly tested to ensure that they are in good order and all tests have to be documented.

110. Materials which can easily catch fire should be disposed of and those documents which are still in use should be stored in a secure place.

111. Activities such as re-wiring, welding or cutting, undertaken as part of structural changes to the premises, should be monitored by ICT staff, so long as there is proof of safety of new wiring required.

112. Clear fire instructions should be available and in the event of fire, these instructions should be followed.

113. Regular fire practices (fire drills) should be conducted.

114. Computer labs should be as much as clean and tidy.

Business Continuity Management

115. The College shall ensure the continuity of its services, especially those involving critical operations, and maintains the availability of information at an acceptable level in the

event of significant disruption.

116. In the event of systems encountering data loss, each system should be covered by a data backup regimen. The media must then be stored both on-site and off-site to limit total loss in case of a declared disaster. The media should contain a copy of specific data as at a specified time. In the event that data is required for recovery, a data restore must be performed from the backup media.

117. System administrators shall ensure that data back-ups must be performed on scheduled basis. Daily backup must be performed automatically for data that changes on a daily basis. Data that is not in the custody of the system administrators, other users will be responsible for backup.

118. Backup must be performed on established schedule for data that change at scheduled intervals, or to respond to major system events.

119. All media, equipment and backup utilities (backup management software and in-house programs) used to perform backups should be tested prior to live use to determine compatibility with computer systems, storage environment, and backup frequencies.

120. In order to ensure ICT service continuity, backup of all critical systems should be in place and maintained by system administrators.

121. Disaster Recovery Site (DRS) should be a real-time based backup site in a remote physical location containing ICT equipment configured and ready to run CBE Systems.

122. The College shall develop and enforce data backup plan and procedures for each application/system.

123. Backup information, together with accurate and complete

records of the backup copies and documented restoration procedures, must be stored in a remote location, at a sufficient distance to avoid being affected by the same disaster that may hit the main site.

124. Backup media must regularly be tested, where practicable, to ensure that they can be relied upon for emergency use when necessary.

125. Restoration procedures must be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.

126. User Data, Database and System state must be backed-up regularly, normally at least twice per day.

127. The contents of the back-up tape/disk must be verified and ensured that the data has been saved. If the backup fails, the process need to be reconfigured and repeated.

128. Backup media must be stored both on-site and off-site. On-site storage is located within a physically secure and fire-proof area.

129. Off-site storage must be in a secure and monitored location physically distant from the source location premises. Authorized Computer department staff responsible for ICT implementation or regulation at CBE should have accesses to this location at any time.

130. Backup and recovery documentation shall be reviewed and updated regularly to account for new technology, business changes, and migration of application to alternative platforms. Documentation of the restoration process must include procedures for the recovery from single- system or application failures as well as for a total data center disaster scenario.

131. Back up documentation should include items necessary to perform essential tasks during a recovery period such as; Identification of all critical data, programs, documentation and support items, clear documentation on how to do the backup and restore, specified period of maximum acceptable outage (MAO) for all systems, backup media storage locations, required backup frequency (e.g. daily, weekly, etc), required backup cycles, backup retention period (as per business and legislative requirements), testing regimen and process and recovery schedule and plan; and location of relevant software and licenses.

132. Computer department shall be responsible for Configuring a fully tested backup system (including media, equipment, and utilities) and data restoration capabilities.

133. Computer department shall be responsible for Initiating, managing, and monitoring all data back-ups.

134. Computer department shall be responsible for ensuring all back-up failures are investigated and examined to ensure process integrity.

135. All electronic data including user's emails should be archived and backed up. The designated system administrator must ensure archiving has been done properly.

136. No archived data should be destroyed without a written approval from the Computer manager.

ICT sustainability issues

137. The College shall mobilize and allocate adequate financial resources for ICT development.

138. To ensure sustainability and auditability of information systems, Free and Open Source Software (FOSS) shall be preferred, promoted and used in the College.

139. Whenever possible the College will use cloud computing solutions for acquisition of ICT services.

140. The Server rooms and computer rooms shall be adequately air conditioned to provide a conducive environment for the ICT equipment.

141. The air conditioners should be serviced regularly to ensure continuous performance.

142. Air conditioning failure should be reported for immediate remedial measures.

143. College shall strive at maintaining more than one ISP to increase availability and reliability of Internet services.

144. College shall regularly undertake preventive maintenance routines to reduce computer systems downtime and repair costs. Systematic inspection, cleaning, and replacement of worn parts, materials, and systems shall be done during the maintenance routines.

Measurement against theft

145. Non CBE employees shall not use CBE ICT resources without prior relevant written permission from authority.

146. Moving ICT equipment owned/leased by CBE outside the premises should follow laid down procedures.

CBE external ICT service Providers

147. All external service providers should be verified by College Computer department as being legitimate before being allowed to access any of the College ICT resources.

148. There shall be a register which will be showing when, why and by whom access was requested and if it was granted or not.

149. External services provider shall complete Confidentiality Agreement Form.

150. In case an external service provider allowed to access systems they should be assigned new login details (username and passwords) and relevant access privileges and not the existing ones.

151. Any created user log on details to allow access to systems should be deactivated as soon as access is no longer required.

152. The contractor shall take all measures to protect from data loss during maintenance operations.

153. All maintenance of ICT equipment and software shall be done at CBE and under the supervision of Computer department personnel. Maintenance shall only be done outside on special permission.

154. In case the damaged ICT equipment needs to be taken to the contractor, the following should be examined: The storage media within the systems shall be removed before the equipment is taken to the contractor. If the storage media is needed, then the sensitivity of data within the media should be examined and for high sensitive the ICT staff shall accompany the contractor.

155. The maintenance of ICT equipment and software shall be allowed where necessary and the login shall be governed by guidelines under "Remote access"

156. Computer department shall ensure that the equipment does not contain sensitive data when hardware is taken by the service provider for servicing or repairing.

157. Service contracts with all service providers including third party vendors should include confidentiality clause and right to have information system audit conducted (internal or external).

158. Prior to entering into an ICT outsourcing arrangement, care should be taken to ensure that process will not compromise the organization objectives, policies and standards. Thus, outsourcing process should base on the following requirements:
    a. Outsourcing activities should consider risks and security concerns.
    b. CBE should develop a contingency plan for critical outsourced technology services to protect them from unavailability of services due to unexpected problems of the technology service provider. This should include termination plan and identification of additional or alternate technology service providers for such support and services.
    c. Outsourced services should be regularly reviewed and analyzed for inappropriate or unusual usage, during the life of the contract.
    d. Any problems discovered during the implementation of the outsourced ICT Services, solutions should be documented and used to improve the controls.
    e. Protection of personal information and organizational data by ensuring appropriate and effective confidentiality agreements are in place.
    f. Compliance with information, security and privacy policies, laws and regulations issues

Information System Audit

159. Purpose of this audit section is to provide guidelines to College security audit team to conduct a security audit on IT based infrastructure system at the College. Audit will be done to protect entire system from the most common security threats which includes: Access to confidential data; Unauthorized access of the department computers; Password disclosure compromise; Virus infections; Open ports, which may be accessed from outsiders (Unrestricted modems unnecessarily open ports).

160. It is the responsibility of ISLC to place an appropriate system of internal audit, which provides an independent assessment

of systems standard operations and security. To execute this, internal audit should be done annually and reports/documents based on these audit should be generated.

161. System administrator or an officer in charge of operations of application systems will be among internal audit team members. He or she will be responsible for supporting IT audit exercise when external audit team visits the College. When requested and for the purpose of performing an audit, any access needed will be provided to members of External Audit team by him/her. This access may include: User level and/or system level access to any computing or communications device; Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on respective system or premises; Access to work areas (labs, offices, server rooms, storage areas, etc.); Access to reports/documents created during internal audit; Access to interactively monitor and log traffic on networks.

Need of approval of cloud computing services

162. College use of cloud computing services must be formally authorized based on the followings:
    a. Cloud Computing services must be approved in writing after certifying that security, privacy, and other Information technology management requirements have been adequately addressed prior to approving the services.
    b. Encryption mechanisms must be used to ensure the authentication, integrity and confidentiality of involved data and communications.
    c. Examine if cloud computing vendor is "Trusted Cloud Computing Vendor".

PART III: COLLEGE WEBSITE GUIDELINES

CBE Website

163. No information that can be damaging to the College's

interest or image shall be displayed on the website of the College including its campuses, departments or any form of a unit.

164. The website shall contain information regarding but not limited to academic matter, research, extension and advisory services, alumni matters, gender issues, curricula issues as well as staff and students' affairs.

CBE Organs and Management

165. The College website shall contain descriptions of various organs including functions, powers, members as well as their qualifications. Organs to be displayed on the website will include the Governing Body (GB), College Academic Board (CAB), the Governing Body Committees, Workers Council, CBEASA, COBESO, Campuses, Centers, Departments and management teams at all levels.

166. Issues approved by office of Public Relations Office for public consumption and in any way they shall not tarnish the image of the College should be uploaded to website.

Advertisements

167. The website being the tool for communication and advertisement shall include advertisements for scholarships, conferences, call for papers, job opportunities, news about decision made by Governing Body and the College Academic Board on various issues, approved research projects under different programmes, Research news, other news and advertisements

Staff Information

168. It is important to include the staff information including their curriculum vitae (CV) in the website so that the visitors can know staff strength including academic, administrative and /or technical staff and their qualifications.

169. Staff information shall include:
    a. The number of academic staff and their curriculum vitae (CV) emphasizing on their list of publications and web links.
    b. The number of administrative staff and their curriculum

vitae (CV).

c. The number of technical staff and their curriculum vitae (CV).
d. Other positions shall also be uploaded as may be required.
e. The list and number of professors
f. The list and number of associate professors
g. The list and number of PhD holders
h. The list and number of masters holders
i. The list and number of bachelor holders

Student Information

170. The website should include information for expected applicants at CBE. This will help prospective students and stakeholders to know the academic programmes offered by CBE and their entry qualifications and other useful information. The information for prospective students shall include the academic programmes offered by CBE and their entry qualifications, information about call for Degree and Non degree programmes - Training Application

171. The number of students enrolled at CBE shall appear on the CBE website. This will help our customers and stakeholders to find out how many students are admitted nationally and internationally.

172. Undergraduate information shall be uploaded on Semester basis and updated regularly. The information shall include
    a. the number of undergraduate students enrolled at CBE,
    b. Percentage of applicants applied for undergraduate studies, female student enrolled both internationally and locally,
    c. applicants admitted into undergraduate studies (both nationally and internationally), students graduated at campus level and College level,
    d. undergraduate students employed after graduation and students awarded scholarships (national or international) after graduations
    e. Ratio of undergraduate students to academic staff shall

be displayed on the website

f. And other useful information

173. Postgraduate information will be entered at least in every six months and updated regularly. This will include:
    a. The number of postgraduate students enrolled at CBE
    b. Percentage of applicants applied for postgraduate studies
    c. Percentage of applicants admitted into postgraduate studies (both nationally and internationally)
    d. Ratio of PhD students graduated to academic staff
    e. Ratio of postgraduate students to academic staff
    f. Percentage of postgraduate fellowships/grants from prestigious bodies awarded to postgraduate via research mode

Teaching and learning issues

174. Teaching and learning information will be displayed on the the College website. The information can include the number of students admitted at CBE each year including educational or academic programmes. The number can be classified by gender and nationality.

175. Academic programmes will be uploaded into the website including
    a. The list and number of academic programmes offered at CBE shall appear in the website.
    b. Honorary degree information indicating the names of the recipients, the year awarded and reason of award is necessary to appear in the website so that they can be accessed by people from different places.

176. The information about student-staff ratio as a reasonable indicator of the workload of the academic staff shall appear in the website. In addition, the trend of the student-staff ratios for some years can help to determine whether the College is improving or not. Ratios shall be in terms of
    a. postgraduate students to academic staff
    b. undergraduate students to academic staff

c. all students to academic members of staff.

177. The achievements for students and staff are indicators of improvement of a College providing good services. The following therefore will be displayed on the website (but not limited to):
    a. The list and number of recognized awards
    b. Technologies developed by CBE
    c. The number of graduates employed after graduation
    d. Staff of the College winning Nobel Prizes and Fields Medals
    e. Alumni of an institution winning Nobel Prizes and Fields Medals
    f. List and number of patents attained
    g. List and number of products commercialized
    h. List and number of technology licensed

Research matters

178. Since research outputs are good indicator of the level of research work at any institution, they will therefore be displayed on the website so that they can be accessed by people from different places. Specifically, this information will include:
    a. Percentage of Academic Staff with PhD or Equivalent and their research experience.
    b. Number, list and description of recognition or awards or stewardship conferred by national and international learned and professional bodies
    c. Percent of funds spent on research
    d. Income generated from services/consultancy

179. Information on research projects will include:
    a. List and number of research projects completed
    b. List and number of research projects in progress
    c. Research funding level at CBE. This shall include funds received through International and National Collaborative Research Grants.
    d. Research grants for academic staff including public, private grants. Consideration on contracted research

whether national or International contract.

180. All publications with their web links shall be published on CBE website including:
    a. List and number of institutional journals at CBE annually and cumulatively
    b. List and number of journal papers published by staff at CBE annually including their web links.
    c. List and number of conference papers published by staff at CBE annually including their web links
    d. List and number of research reports published by staff at CBE annually including their web links.
    e. List and number of books published at the CBE by its staff
    f. Sponsored symposia/Seminars/ Workshops and conferences organized nationally and internationally including the web links of their proceedings.

181. All information related to consultancy shall be displayed on the website.

182. List and names of outreach activities made should be displayed on the website

Facilities and services

183. The information about equipment that are fully operational and calibrated or physical facilities and supporting facilities available at the College shall be published on the College website.
    a. Library facilities
        i. Number of books and journals present in the Library including e-journals.
        ii. Amount spent on library as percentage of the total budget
        iii. Number of visits to the Library and trends
        iv. Library loan and inter-library loan services
        v. Electronic resources services
        vi. Information search services
        vii. Any other services available
    b. ICT services
        i. Number of personal computers available for

academic staff

ii. The ratio of personal computers to academic staff

iii. Number of academic staff with computers connected to the Internet

iv. Any other ICT service available

c. Laboratory information shall include:

i. Description and information about Laboratories of Campuses, Directorates, Departments, and units should be uploaded on the website including; Services offered; Laboratory facilities; and Name and number of laboratories for practical

184. Health Information shall be displayed on the website such facilities will include but not limited to:

a. Description and information about Health
b. Services offered
c. Health facilities
d. Name and number of Health centers available.

185. Sports and Clubs information shall be displayed on the website such facilities will include but not limited to:

a. Number of teams participating in the SHIMIVUTA games
b. Position of the College in the previous SHIMIVUTA competition

Alumni and / or Famous People Who Had Affiliation with CBE

186. Alumni and or famous people who had affiliated with CBE shall be displayed on the website including list of their names and their qualification, Post held all over the world, the year graduated from CBE should be uploaded on the website.

Associations and Trade Unions

187. Information about trade unions and associations available at CBE such as CBEASA, COBESO, RAAWU and THTU which are meant to help CBE community shall be displayed on the website. Information that will be uploaded shall include the associations'/unions' role, services and ways to join.

Links to CBE Partners, Allied Ministries and Other Institutions

188. There shall be links to developmental partners and collaborators, allied ministries such as Ministry of Industry, Trade and Investment, and any institution that has direct relationship of any kind.

Formatting Website Contents

189. The web format and content must be consistent with the purpose of College of Business Education website. Furthermore, the website contents must rely on Acceptable Use Policies, ICT Policy and Guidelines.

190. The following are guidelines on further formatting the contents:

a. Complex sentence structures shall be avoided and it will include just one idea or concept per sentence.
b. Use active ahead of passive words. For example, 'We plant crops to protect our environment' is shorter and easier to comprehend than, 'The crops are planted by us to protect our environment'.
c. The language shall be suitable to intended audiences
d. Make a site with a clear hierarchy and text links. Every page shall be reachable from at least one static text link.
e. The content shall use text instead of images to display important names, content, or links since most of web crawlers do not recognize text contained in images.
f. Bold important words to help users locate information quickly and easily.
g. It is highly recommended that stakeholders adopt the use of shorter words where possible. For example, use 'begin' rather than 'commence', 'used to' rather than 'accustomed to'.
h. It is highly recommended to;
    i. Avoid slang or jargon
    ii. Limit each paragraph to one idea
i. The first line of each paragraph should contain the conclusion for that paragraph,

j. The opening paragraph on every page should always contain the conclusion of that page.
k. Use descriptive sub-headings
l. Bold the important words
m. Use descriptive link text
n. Use lists
o. Use left-aligned text
p. Observe spelling and grammar
q. Check page texts for accuracy before posting
r. Uploaded images in standard that shall load correctly within a short time.
s. Large images shall not be required
t. The office responsible for a page shall be displayed with contact information in the "Contact Us" box of the website home page.
u. Indicate the date that every page was last updated
v. All CBE web pages shall be constructed using the standard CBE web templates or content management systems using style sheets, and supporting graphics shall be compatible with those standards.

College Website Committee

191. There shall be a College website committee (CWC) which shall regularly report to the Information Systems and Library Services Committee on website matters.

192. CWC shall be chaired by Deputy Rector – Academic, Research and Consultancy.

193. The CWC shall be constituted by
a. Computer manager.
b. All website chairpersons of website content committees (WCC) across College units (academic and administrative).
c. Webmaster who should be an online communication specialist from publicity and marketing department who will be the secretariat of CWC.
d. Public Relations Officer
e. Librarian

f. Members of Website Technical Committee

194. The duties and responsibilities of CWC include:
   a. To ensure that CBE Website is in good shape in terms of general appearance, user-friendly and regularly updated content.
   b. To develop and update guidelines and/or formats for the information required to appear on various units of the College
   c. To ensure that information on all Web pages on CBE Website is updated regularly and accordingly.
   d. CWC shall monitor, evaluate and instruct accordingly.
   e. College website Committee (UWC) shall approve the ranking of websites of College units

Website Content Committees at the College

195. There shall be website content committees (WCC) in all academic and administrative departments at all levels in the College.

196. WCC shall be composed of at least three members appointed by heads of the respective department/unit

197. WCC shall be chaired by the Head of the respective department/unit or his/her appointee.

198. WCC shall have the following duties and responsibilities:
   a. soliciting, collecting, reviewing, endorsing and uploading Web contents for units/sections under their jurisdiction
   b. ensuring that updating of Web page contents is done at least monthly
   c. Liaising with the webmaster on various matters related to website
   d. Generating quarterly and annual reports and present their deliberations to CWC. Reports shall show the previous and current status

All units to

199. All College units shall make the website matters a

have a permanent item of agenda

permanent item of agenda in their meetings. This can go hand in hand with administrative incentives for website content committees.

Ranking of units websites

200. Ranking of websites of College department/units shall be done at least once per quarter. Ranking announcements will be posted to CBE website and other places. Department/Unit websites ranking at the top will be given priority to appear on the front page. In doing this it is expected to assist in (a) revealing the best College units in producing content (b) raising awareness that contents are produced by staff and departments. Furthermore, the department/units that will be ranking last for consecutive of two years will be given warning letters.

201. The ranking process shall follow the world-wide used criteria including:

(i) Size of the website which refers to number of pages;
(ii) Visibility which is the number of external links received (back links) by the number of referring domains of that back links;
(iii) Number and quality of rich files in the website.
(iv) Number/ratio of publications available on website including those in the institutional repositories and Google Scholar. Details of these criteria shall be revised by CWC from time to time.

202. There shall be prizes in terms of trophy or other recognition way as deemed appropriate by the management for best websites of units based on four scores obtained in a year. The value of the prizes shall be reviewed from time to time and approved by relevant College organs.

information for Learning and Teaching Technologies

203. College staff or any user of ICT resources shall not upload copies of copyrighted materials.

204. Student Personal identifiable information must be kept

confidential. Confidential information includes: student ID and other identification numbers, biographical information, such as home address and telephone number, personal e-mail address, educational history including classes taken or enrolled in, assessments or opinions about the student including marks and grades, bursaries, or awards, photographs, health information.

205. CBE shall strive to ensure student information are kept in secure facilities and equipment, locked rooms and password protected computer systems accessible only to staff whose work requires them to have access.

206. Any security breach of student information (such as unauthorized access or disclosure, the loss or theft of files, laptops, or flash drives containing student information, or misdirected e-mail, etc.) must be reported immediately to the appropriate College relevant authorities.

207. Access to student information shall only be limited to staff who need the information to do their job.

208. Students do not have the right to access the personal information of individuals other than themselves. Returning assignments or exams to students or posting grades must be done in a way which does not reveal personal information to other students.

209. Electronic posting of student personal information (including photographs) on publicly available websites (including social media sites e.g. Facebook) or websites available to campuses, staff, and students requires prior notice to the students who must consent to the use of their personal information in this way.

210. CBE shall keep students' personal information for a minimum of three years after graduation. Beyond that student information must be kept only as long as necessary

to complete the contractual obligations between the College and the student (for example to provide information on the academic achievements of the student to employers, educational institutions, licensing/regulatory bodies, and to the student him/herself, and to provide the student with appropriate support and other services).

BREACH OF GUIDELINE

211. Any person who contravenes these guidelines commits offense(s) and shall be liable to punishments accordance with Staff Regulations, or staff by laws and or national and international laws.

Bibliography

1. College of Business Education, Information and Communication Technology (ICT) Policy (2017).
2. The Cybercrimes Act, (2015)
3. The Electronic Transactions Act, 2015,
4. College of Business Education, Guidelines for Website Contents, (2018).
5. College of Business Education, Staff Regulation, (2013).
6. The United Republic of Tanzania - Ministry of Finance, ICT Security Guidelines, December 2012.
7. Republic of Malawi, Public Service ICT Standards, January 2014.
8. Michigan State College, Faculty and Staff Guide to Computing and Technology, 2010/11.

Appendices

Appendix 1

College of Business Education
Network Access confidentiality Form

User Details

Access required to Network/System/Application

New User [ ] Existing User [ ] Deletion of User [ ]

Full Name_____ PF No._____

JobTitle_____Department/School/Campus_____

Cell Phone Number _____Email Address_____

Access required to function (s) _____

Authority Level where applicable _____

I acknowledge that:

- My Password will at all times remain confidential to me
- I will take all necessary precautions to ensure that no unauthorized persons can gain access to my password
- Failure to adhere to the above mentioned will be viewed as a serious breach of trust and will result severe disciplinary action.

Signature _____

Authorizing Officer

Full Name.....Department.....

Work telephone number..... Job Title.....

Cell Phone Number _____

Email Address _____

I confirm that the access required is in the accordance with the user's job description.

Signature: _____

Appendix 2

CBE ICT Facility Borrowing Application Form

ICT Facilities are available for College staff to borrow for CBE work related purposes. Maximum loan time is one week or more in approved special case.

Please note, damage, or loss of the item will result in the corresponding charge being assessed to the individual or department making the booking.

The ICT facility may be borrowed for the following reasons:

- On Campus Meetings • CBE Community Events (e.g. Public Lectures, Open Day)
- Failure of work computer

The ICT Facility shall not be borrowed in the following circumstances:

• Conference Attendance ( ) • Overseas Travel ( ) • Personal Home Use ( )

Authorization must be obtained from your head of Department or unit. Costs associated with any damage or loss of the laptop will be billed to the Department/unit in CBE.

Dates Required: From: ----/-----/----- To: ----/-----/-----

<u>SECTION ONE</u> ***(TO BE COMPLETED BY THE APPLICANT)***
Full Name: .....

Position: ..... Dept/Unit:
.....

Reason for Borrowing:

.....

Location Where the ICT facility will be used

Mobile Number..... Signature:..... Date:.....

<u>SECTION TWO</u> ***(TO BE COMPLETED BY THE AUTHORISING OFFICER)***

Authorization

(To be completed by Head of Department/Unit)

The above staff member is authorized to borrow the nominated ICT facility for the period specified. The Department/Unit will meet the associated costs if the item is damaged or lost.

Full Name:…… Position:……

Dept/Unit:……

Signature: …… Date: ……

Computer Manager Comments

Comments:
……
……

Signature: ……
Date……

Appendix 3

College of Business Education

Change Request Form

Change Request #: _____Department/Unit: _____

CHANGE REQUEST INITIATION: Originator: _____

Phone#: _____ _____Date Submitted: ____/____/____

System/Product/Service Name: _____ Version Number: _____

CONFIGURATION ITEM:

Software: ___ Firmware: ___ Hardware: ___ Documentation: ___

Other: _____

CHANGE TYPE:

New Requirement: ___ Requirement Change: ___ Design Change: __

Other: _____

REASON:

Legal: ___ Market: ___ Performance: ___ Customer Request: ___Defect: _____

Other: _____

PRIORITY:

Emergency: _____ Urgent: _____ Routine: _____D***ate Required:***

_____/_____/_____

CHANGE DESCRIPTION: *(Detail functional and/or technical information. Use attachment if necessary.)*

Attachments:Yes / No

TECHNICAL EVALUATION: *(Use attachment to explain changes, impact on other entities, impact on performance etc.)*

Received By:_____Date Received: ___/___/___

Assigned To:_____Date Assigned: ___/___/___

Type of Software/Hardware/etc.

Affected_____
_____

Modules/Screens/Tables/Files Affected:

_____
__

APPROVALS: Change Approved: _____ Change Not Approved: _____

Hold (Future Enhancement): _____

1. Approved By::_____

Signature _____Date: ____/____/____

College of Business Education

Computer Department

User Support Form

Section 1: To be filled by End-User/Department

Name:	**Reported Problem:** Please Tick Appropriate	**Provide problem brief description**
Department Name:	Computer/Laptop ☐	
Building/Room:	Internet/Network ☐	
Phone number:	Email ☐	
Email:	Software/Application (MS Word, SARIS) ☐	
Request Date:	Virus ☐	
Request Time:	Login Failure ☐	
	Printer ☐	
	Projector ☐	
	Other: Please mention	

Section 2: To be filled by Computer Department/Help Desk

Job No:	Name of Technical Personnel:	Date:

Section 3: To be filled by Technical personnel on completion of the job.

Problem cause:	Solution details:	Cost (if any)

Section 4: User department details

I confirm that the technician/group worked on the problem described above.

Client
Name:_____Signature_____Date:_____