Bugema University ICT Support Department

Policy and Procedure Manual

POLICY NUMBER: BU/ITSP/1.0

POLICY DATE: June/2020

REVIEW PERIOD: 1 year

REVIEW RECORD: Next review date June 2021

Table of Contents

Introduction

The Bugema University ICT Support Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the institution which must be followed by all staff and students. It also provides guidelines Bugema University will use to administer these policies, with the correct procedure to follow.

Bugema University will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures.

Any suggestions, recommendations or feedback on the policies and procedures specified in this manual can university main reception.

These policies and procedures apply to all employees, students and visitors.

Technology Hardware Purchasing Policy

Computer hardware refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and RAM. External hardware devices include monitors, keyboards, mice, printers, and scanners.

Purpose of the Policy

This policy provides guidelines for the purchase of hardware for the institution to ensure that all hardware technology for the institution is appropriate, value for money and where applicable integrates with other technology for the institution. The objective of this policy is to ensure that there is minimum diversity of hardware within the institution.

Procedures

Purchase of Hardware

Purchasing desktop computer systems

The desktop computer systems purchased must run a minimum of Windows 7 or Linux operating systems and integrate with existing hardware of the Institution severs.

The desktop computer systems must be purchased as standard desktop system bundle and should be compatible to the most recent technology on market.

Any change in requirements must be authorised by Head, ICT Support Department

All purchases of desktops must be supported by 1 Year warranty and be compatible with the institution’s server system.

All purchases for desktops must be in line with the purchasing policy in the financial policies and procedures manual.

Purchasing portable computer systems

The purchase of portable computer systems includes portable devices such as notebooks, laptops, tablets, IPad etc.

Portable computer systems purchased must run a relevant genuine operating system e.g. Windows, Android, IOS, etc. and integrate with existing server hardware

Any change in the above requirements must be authorised by Head, ICT Support Department

All purchases of all portable computer systems must be supported 1 Year warranty and compatible with the institution’s server system.

All purchases for portable computer systems must be in line with the purchasing policy in the financial policies and procedures manual.

Purchasing server systems

Server systems can only be purchased by ICT Support department

Server systems purchased must be compatible with all other computer hardware in the institution.

All purchases of server systems must be supported by 1 year warranty and be compatible with the institution's server systems.

Any change from the above requirements must be authorised by Head, IT Support department

All purchases for server systems must be in line with the purchasing policy in the financial policies and procedures manual.

Purchasing computer peripherals

Computer system peripherals include computer spare parts, printers, scanners, external hard drives, flash drives, VGA/VDI cables, keyboards

Computer peripherals can only be purchased where they are not included in any hardware purchase or are considered to be an additional requirement to existing peripherals.

Computer peripherals purchased must be compatible with all other computer hardware and software in the institution.

The purchase of computer peripherals can only be authorised by Head, IT Support department

All purchases of computer peripherals must be supported by 1 year warranty and be compatible with the institution's other hardware and software systems.

Any change from the above requirements must be authorised by Head, ICT Support department

All purchases for computer peripherals must be in line with the purchasing policy in the financial policies and procedures manual.

Policy for Getting Software

Purpose of the Policy

This policy provides guidelines for the purchase of software for the institution to ensure that all software used by the institution is appropriate, value for money and where applicable integrates with other technology for the institution. This policy applies to software obtained as part of hardware bundle or pre-loaded software.

Procedures

Request for Software

All software, including non-commercial software such as open source, freeware must be approved by Head, ICT Support department prior to the use or download of such software.

Purchase of software

The purchase of all software must adhere to this policy.

All purchased software must be purchased by ICT Support department

All purchases of software must be supported by 1 year warranty and be compatible with the institution's server and/or hardware system.

Any changes from the above requirements must be authorised by ICT Support department.

Open source or freeware software can be obtained without payment and usually downloaded directly from the internet.

In the event that open source or freeware software is required, approval from ICT Support department must be obtained prior to the download or use of such software.

All open source or freeware must be compatible with the institution's hardware and software systems.

Any change from the above requirements must be authorised by ICT Support department.

Policy for Use of Software

Purpose of the Policy

This policy provides guidelines for the use of software for all employees within the institution to ensure that all software use is appropriate. Under this policy, the use of all open source and freeware software will be conducted under the same procedures outlined for commercial software.

Procedures

Software Licensing

All computer software copyrights and terms of all software licenses will be followed by all employees and students of the institution.

Where licensing states limited usage (i.e. number of computers or users etc.), then it is the responsibility of ICT Support department to ensure these terms are followed.

ICT Support department is responsible for completing a software audit of all hardware twice a year to ensure that software copyrights and license agreements are adhered to.

Software Installation

All software must be appropriately registered with the supplier where this is a requirement. Bugema University is to be the registered owner of all software.

Only software obtained in accordance with the software policy is to be installed on the institution's computers.

All software installation is to be carried out by ICT Support department

A software upgrade shall not be installed on a computer that does not already have a copy of the original version of the software loaded on it.

Software Usage

Only software purchased in accordance with the software policy is to be used within the institution.

Prior to the use of any software, the employee must receive instructions on any licensing agreements relating to the software, including any restrictions on use of the software.

Employees are prohibited from bringing software from home and loading it onto the institution's computer hardware.

Unless express approval from ICT Support department is obtained, software cannot be taken home and loaded on employees' home computer

Where an employee is required to use software at home, an evaluation of providing the employee with a portable computer should be undertaken in the first instance. Where it is found that software can be used on the employee's home computer, authorisation from ICT Support

department is required to purchase separate software if licensing or copyright restrictions apply. Where software is purchased in this circumstance, it remains the property of the institution and must be recorded on the software register by ICT Support department

Unauthorised software is prohibited from being used in the institution. This includes the use of software owned by an employee and used within the institution.

The unauthorised duplicating, acquiring or use of software copies is prohibited. Any employee who makes, acquires, or uses unauthorised copies of software will be referred to Human resource department for further consultation.
The illegal duplication of software or other copyrighted works is not condoned within this institution and Human resource department is authorised to undertake disciplinary action where such event occurs.

Bring Your Own Device Policy

At Bugema University we acknowledge the importance of mobile technologies in improving institution communication and productivity. In addition to the increased use of mobile devices, staff members have requested the option of connecting their own mobile devices to Bugema University's network and equipment. We encourage you to read this document in full and to act upon the recommendations. This policy should be read and carried out by all staff.

Purpose of the Policy

This policy provides guidelines for the use of personally owned notebooks, smart phones, tablets and any other types of mobile devices for institution purposes. All staff who use or access Bugema University's technology equipment and/or services are bound by the conditions of this Policy.

Each employee who utilizes personal mobile devices agrees:

Not to download or transfer institution or personal sensitive information to the device. Sensitive information includes institution or personal information that you consider sensitive to the institution, for example intellectual property, other employee details etc.

Not to use the registered mobile device as the sole repository for Bugema University's information. All institution information stored on mobile devices should be backed up

To make every reasonable effort to ensure that Bugema University's information is not compromised through the use of mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorised persons and all registered devices should be password protected

To maintain the device with maintenance requirements of mobile devices such as current operating software, current security software etc.

Not to share the device with other individuals to protect the institution data access through the device

To abide by Bugema University's internet regulations for appropriate use and access of internet sites etc.

To notify Bugema University immediately in the event of loss or theft of the device

Not to connect USB memory sticks from an untrusted or unknown source to Bugema University's equipment.

All employees who have a registered personal mobile device for institution use acknowledge that the institution:

Owns all intellectual property created on the device

Can access all data held on the device, including personal data

Will regularly back-up data held on the device

Will delete all data held on the device in the event of loss or theft of the device

Has first right to buy the device where the employee wants to sell the device

Will delete all data held on the device upon termination of the employee. The terminated employee can request personal data be reinstated from back up data

Has the right to deregister the device for institution use at any time. Keeping mobile devices secure

The following must be observed when handling mobile computing devices (such as notebooks and iPads):

Mobile computer devices must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle, even if it is locked. Wherever possible they should be kept on the person or securely locked away.

Cable locking devices should also be considered for use with laptop computers in public places, e.g. in a seminar or conference, even when the laptop is attended

Mobile devices should be carried as hand luggage when travelling by aircraft.

Security Policy

Purpose of the Policy

The purpose of the ICT Security Policy is to ensure business continuity and to minimise operational damage by reducing the impact of security incidents.

Scope

This Policy applies in respect of all ICT-related systems, hardware, services, facilities and processes owned or otherwise made available by the Bugema University or on its behalf, or which are connected to the University network and servers, including for the avoidance of doubt any personally-owned devices that are used in connection with University activities (together, **I.T. Systems**).

The threats we face

The University is facing increasing security threats from a wide range of sources. Systems and networks may be the target of a variety of attacks, including computer based fraud, surveillance or vandalism. Such threats to I.T. security are generally expected to become more widespread, more ambitious and increasingly sophisticated.

Because of increasing dependence on I.T. systems and services, the University is becoming more vulnerable to security threats. The growth of networking, cloud services and mobile devices presents new opportunities for unauthorised access to computer systems or data and reduces the scope for central, specialised control of I.T. facilities.

Procedures

Physical Security

For all servers, mainframes and other network assets, the area must be secured with adequate ventilation and appropriate access through security measures such as keypad, lock etc.

It will be the responsibility of ICT Support department to ensure that this requirement is followed at all times. Any employee becoming aware of a breach to this security requirement is obliged to notify ICT Support department immediately.

All security and safety of all portable technology, such as laptop, notepads, iPad etc. will be the responsibility of the employee who has been issued with the laptop, notepads, iPads, mobile phones etc. Each employee is required to use secure locks, passwords, etc. And to ensure the asset is kept safely at all times to protect the security of the asset issued to them.

In the event of loss or damage, ICT Support department will assess the security measures undertaken to determine if the employee will be required to reimburse the institution for the loss or damage.

All laptops, notepads, iPads etc. when kept at the office desk is to be secured by the relevant security measures such as keypad, lock etc. provided by ICT Support department.

Information Security

All the relevant data to be backed up - either general such as sensitive, valuable, or critical institution data is to be backed-up.

It is the responsibility of ICT Support Department to ensure that data back-ups are conducted regularly and the backed up data is kept either on cloud, offsite venue, employees home etc.

All technology that has internet access must have anti-virus software installed. It is the responsibility of ICT Support department to install all anti-virus software and ensure that this software remains up to date on all technology used by the institution.

Disposal of equipment

When permanently disposing of equipment containing all types of storage media (including removable media) all sensitive or confidential data and licensed software should be irretrievably deleted during the disposal process. Damaged storage devices containing sensitive or confidential data will undergo assessment to determine if the device should be destroyed, repaired or discarded. Such devices will remain the property of the University and only be removed from site with the permission of the information asset owner.

Sensitive or confidential information

Sensitive or confidential data may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured. Sensitive or confidential data should only be accessed from equipment in secure locations and files must never be printed on a networked printer that does not have adequate protection or security.

Use of electronic communication

The identity of online recipients, such as email addresses and fax numbers should be checked carefully prior to dispatch, especially where the information content is sensitive or confidential. Information received electronically must be treated with care due to its inherent information security risks. File attachments should be scanned for possible viruses or other malicious code.

Sensitive or confidential information should only be sent electronically (e.g. by email) to external recipients when it is encrypted or protected by a password.

Access to personal or individual data for systems management purposes

Some individuals may need access to personal data identifying individuals, or to data which belongs to others, in order to manage systems or to fix problems. These individuals will be required to sign a data protection declaration before they are sanctioned to carry out these duties.

Travelling

Devices must be provided with an appropriate form of access protection such as a password or encryption to prevent unauthorised access to their contents. In addition, more recent means of authentication such as Touch-ID or Face ID are also acceptable forms of access protection.

Equipment and media should not be left unattended in public places and portable devices should be carried as hand luggage. To reduce the opportunities for unauthorised access, automatic shutdown features should be enabled. Passwords or other similar security tokens for access to the University's systems should never be stored on mobile devices or in their carrying cases. Screens on which sensitive or confidential information is processed or viewed should be fitted with a privacy filter or be sited in such a way that they cannot be viewed by unauthorised persons.

Export and import controls apply when travelling to certain countries which restrict the use of encrypted devices. Advice should be taken from ICT Support before any travel arrangements are made.

All external suppliers who have access to University I.T. Systems or data must work under the supervision of University staff and in accordance with this Policy. A copy of the Policy will be made available to the supplier, if required.

All information used within the institution is to adhere to the privacy laws and the institution's confidentiality requirements. Any employee breaching this will be penalized.

Building access control

Areas and offices where sensitive or confidential information is processed will be given an appropriate level of physical security and access control. Line managers will provide information on the potential security risks and the measures used to control them to staff with authorisation to enter such areas.

Operational procedures

System owners must ensure that the procedures for the operation and administration of the University's business systems and activities are documented and that those procedures and documents are regularly reviewed and maintained. Duties and areas of responsibility must be segregated to reduce the risk and consequential impact of I.T. security incidents that might result in financial or other material damage to the University.

Procedure for reporting of concerns

System owners must ensure that procedures are established and widely communicated for the reporting to IT Support of security incidents and suspected security weaknesses in the University's I.T. Systems. They must also ensure that mechanisms are put in place to monitor and learn from those incidents. Procedures must be established for the reporting of software malfunctions and faults in the University's I.T. Systems. Faults and malfunctions must be logged and monitored and timely corrective action taken.

Change management

Changes to operational procedures or hardware must be controlled to ensure continuing compliance with the requirements of this Policy and must have management approval. Development and testing facilities for business critical systems will be separated from operational facilities and the migration of software from development to operational status will be subject to formal change control procedures. Acceptance criteria for new information systems, upgrades and new versions will be established and suitable tests of the system carried out prior to migration to operational status. Tests involving live data or periods of parallel running may only be permitted where adequate controls for the security of the data are in place. Procedures will be established to control the development or implementation of all operational software, which must be approved by the University administration before introduction and a Privacy Impact Assessment must be completed and approved by the Records Management Service for any new system that will involve the processing of personal data. All systems developed for or within the University must follow a formalised development process.

Risk assessment

The security risks to the information assets of all system development projects will be assessed by system owners and access to those assets will be controlled

Service level agreements

Any facilities management, outsourcing or similar company with which the University may do business must be able to demonstrate compliance with the University's ICT Support Security Policy and must enter into binding service level agreements that specify the performance to be delivered and the remedies available in case of non-compliance.

Access control standards

System owners must establish appropriate access control standards for all information systems which minimise information security risks yet allow the University's business activities to be carried out without undue hindrance. Access to all systems must be authorised by the manager responsible for the system and a record must be maintained of such authorisations, including the appropriate access rights or privileges granted. Procedures must be established for all information systems to ensure that users' access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, staff change their role, or staff or students leave the organisation. Users' access rights must be reviewed at regular intervals.

Starters, Leavers and Affiliates

Line managers must ensure that access to I.T. Systems is only available to employees during their period of employment. In particular, line managers must ensure that the system access of leavers is withdrawn as soon as employment is terminated. Those requesting Affiliate status must ensure that system access does not extend beyond the requirements of the Affiliate's activities. Those requesting Affiliate status must also ensure that system access is withdrawn as soon as the Affiliate's relationship with the University ceases.

Risk assessment and management

System owners must ensure that the information assets associated with any proposed new or updated systems are identified, classified and recorded, and a risk assessment, including, where relevant, a privacy impact assessment, is undertaken to identify the probability and impact of security failure. Equipment supporting business systems must be given adequate protection from unauthorised access, environmental hazards and electrical power failures.

Access control

System owners must ensure that access controls are maintained at appropriate levels for all I.T. Systems and that any changes of access permissions are authorised by the manager of the system or application. A record of access permissions granted must be maintained. Access to all I.T. Systems must use a secure login process and access may also be limited by time of day or by the location of the initiating terminal, or both.

System owners must ensure that all access to systems containing sensitive or confidential information is logged to identify potential misuse of systems or information. They must also ensure that password management procedures are put into place to ensure the implementation of security procedures and to assist users in complying with best practice guidelines.

Remote access to the network must be subject to robust authentication as well as appropriate levels of security. Virtual Private Network, wireless, and other connections to the network are only permitted for authorised users.

Access to operating system commands must be restricted to those persons who are authorised to perform systems administration or management functions. Use of such commands should be logged and monitored.

Change management

System owners must ensure that the procurement or implementation of new or upgraded software is carefully planned and managed and that any development for or by the University always follows a formalised development process with appropriate audit trails. Information security risks associated with such projects must be mitigated using a combination of procedural and technical controls. Business requirements for new software or enhancement of existing software must specify the requirements for information security controls.

The implementation, use or modification of all software on the University's business systems must be controlled. All software must be checked before implementation to protect against malicious code.

All changes must be properly tested and authorised before moving to the live environment.

Network design

Computing and Library Services must ensure that the University data and telecoms network is designed and configured to deliver high performance and reliability to meet the University's needs whilst providing a high degree of access control and a range of privilege restrictions. Appropriately configured firewalls or other security devices must be used to protect the networks supporting the University's business systems.

Logging

System owners must ensure that security event logs, operational audit logs and error logs are properly reviewed and managed by qualified staff. System clocks must be regularly synchronised between the Universities's various processing platforms.

Password Policy

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of Bugema University's entire network. As such, all Bugema university employees including contractors and vendors with access to Bugema University systems are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Bugema University facility and has access to the Bugema University network.

Policy

General

• All systems-level passwords (e.g., root, enable, network administrator, application administration accounts, etc.) must be changed at least every 90 days.

• All production system-level passwords must be part of the Information Security administrated global password management database.

• All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 90 days and cannot be reused the past 10 passwords.

• User accounts with access to system admin privileges must have a unique password from all other accounts held by that user.

• Passwords must not be inserted into email messages or other forms of electronic communication.

• All user-level, system-level passwords must conform to the guidelines described below.

Guidelines

Password Construction Requirements

i. Be a minimum length of eight (8) characters on all systems.

ii. Not be a dictionary word or proper name.

iii. Not be the same as the User ID.

iv. Expire within a maximum of 90 calendar days.

v. Not be identical to the previous ten (10) passwords.

vi. Not be transmitted in the clear or plaintext outside the secure location.

vii. Not be displayed when entered.

viii. Ensure passwords are only reset for authorized user.

Password Deletion

All passwords that are no longer needed must be deleted or disabled immediately. This includes, but is not limited to, the following:

• When a user retires, quits, is reassigned, released, dismissed, etc.

• Default passwords shall be changed immediately on all equipment.

• Contractor accounts, when no longer needed to perform their duties.

When a password is no longer needed, the following procedures should be followed

• Employee should notify his or her immediate supervisor.

• Contractor should inform his or her point-of-contact (POC).

• Supervisor or POC should fill out a password deletion form and send it to.

• ICT Support department will then delete the user's password and delete or suspend the user's account.

• A second individual from that department will check to ensure that the password has been deleted and user account was deleted or suspended.

• The password deletion form will be filed in a secure filing system.

Password Protection Standards

Do not use your User ID as your password. Do not share Bugema University passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Bugema University information.

Here is a list of "do not's"

• Don't reveal a password over the phone to anyone

• Don't reveal a password in an mail message

• Don't reveal a password to the boss

• Don' talk about a password in front of others

• Don't hint at the format of a password (e.g., "my family name")

• Don't reveal a password on questionnaires or security forms

• Don’t share a password with family members

• Don’t reveal a password to a co-worker while on vacation

• Don’t use the "Remember Password" feature of applications

• Don’t write passwords down and store them anywhere in your office.

• Don’t store passwords in a file on ANY computer system unencrypted.

If someone demands a password, refer them to this document.

If an account or password is suspected to have been compromised, report the incident to ICT Support department and change all passwords.

Application Development Standards

Application developers must ensure their programs contain the following security precautions:

• Should support authentication of individual users, not groups.

• Should not store passwords in clear text or in any easily reversible form.

• Should provide some sort of role management, such that one user can take over the function of another without having to know the other’s password.

• Should support Terminal Access Controller Access Control System+ (TACACS+), Remote Authentication Dial-In User Service (RADIUS), and/or X.509 with Lightweight Directory Access Protocol (LDAP) security retrieval, wherever possible.

Remote Access Users

Access to the Bugema University networks via remote access is to be controlled by using either a Virtual Private Network (in which a password and user id are required) or a form of advanced authentication (i.e., Biometrics, Tokens, Public Key Infrastructure (PKI), Certificates, etc.).

Penalties

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

User Account – Access Validation Policy

Purpose

To establish requirements for user accounts and access validation for all Bugema University networks to ensure the security of system access and accountability.

Scope

All accounts shall be reviewed annually by the ICT Support Administrator/System Administrator or his/her designee to ensure that access and account privileges commensurate with job functions, need-to-know, and employment status on systems that contain Bugema University Information. The System Administrator or his/her designee may also conduct periodic reviews.

Policy

All guest accounts (for those who are not official employees of Bugema University) with access to the Bugema University network shall contain an expiration date of one year or the work completion date, whichever occurs first. All guest accounts (for private contractor personnel) must be sponsored by the appropriate authorized member of the administrative entity managing the resource.

The System Administrator or his/her designee should disable all new accounts that have not been accessed within 30 days of creation. Accounts of individuals on extended leave (more than 30 days) should be disabled. (Note: Exceptions can be made in cases where uninterrupted access to IT resources is required. In those instances, the individual going on extended leave should have a manager-approved request from the designated account administrator or assistant.) The System Administrator or his/her designee must be notified if a user's information system usage or need-to-know changes (i.e., the employee is terminated, transferred, etc.). If an individual is assigned to another office for an extended period (more than 90 days), the System Administrator or his/her designee will transfer the individual’s account(s) to the new office.

The System Administrator or his/her designee will remove or disable all access accounts for separated or terminated employees immediately following separation from the agency. Primary responsibility for account management belongs to the System Administrator or his/her designee. The System Administrator or his/her designee shall:

- Modify user accounts in response to events like name changes, accounting changes, permission changes, office transfers, etc.

- Periodically review existing accounts for validity, and -- Cooperate fully with an authorized security team that is investigating a security incident or performing an audit review.

Penalties

Any violation of this policy may result in network removal, access revocation, corrective or disciplinary action, and termination of employment.

Website Policy

Purpose of the Policy

This policy provides guidelines for the maintenance of all relevant technology issues related to the institution website.

Procedures

Website Register

The website register must record the following details:

List of domain names registered to the institution

Dates of renewal for domain names

List of hosting service providers

Expiry dates of hosting

The keeping the register up to date will be the responsibility of ICT Support department. ICT Support department will be responsible for any renewal of items listed in the register.

Website Content

All content on the institution website is to be accurate, appropriate and current. This will be the responsibility of the quality assurance department.

The content of the website is to be reviewed monthly.

The following persons are authorized to make changes to the institution website:

1. The university webmaster
2. ICT Support department
3. Quality assurance department

Basic branding guidelines must be followed on websites to ensure a consistent and cohesive image for the institution.

IT Service Agreements Policy

Purpose of the Policy

This policy provides guidelines for all IT service agreements entered into on behalf of the institution.

Procedures

The following IT service agreements can be entered into on behalf of the institution:

Provision of general IT services

Provision of network hardware and software

Repairs and maintenance of IT equipment

Provision of institution software

Provision of mobile phones and relevant plans

Website design, maintenance etc.

Internet/ Voice services

All IT service agreements must be reviewed by the university administration committee before the agreement is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by one of the university top administrators.

All ICT service agreements, obligations and renewals must be recorded.

Where an ICT service agreement renewal is required, in the event that the agreement is substantially unchanged from the previous agreement, then this agreement renewal can be authorized by finance manager.

Where an ICT service agreement renewal is required, in the event that the agreement has substantially changed from the previous agreement, administration must be consulted before the renewal is entered into.

Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by one of the top administrators

In the event that there is a dispute to the provision of ICT services covered by an ICT service agreement, it must be referred to Bugema university administrator who will be responsible for the settlement of such dispute.

Emergency Management of Information Technology

Purpose of the Policy

This policy provides guidelines for emergency management of all information and communication technology within the institution.

Procedures

IT Hardware Failure

Where there is failure of any of the institution's hardware, this must be referred to ICT Support department immediately.

It is the responsibility of ICT Support department to relevant actions that should be undertaken in the event of IT hardware failure.

It is the responsibility of ICT Support department to undertake tests on planned emergency procedures quarterly to ensure that all planned emergency procedures are appropriate and minimize disruption to institution operations.

Virus or other security breach

In the event that the institution's information technology is compromised by software virus or

Ransom ware such breaches are to be reported to ICT Support department immediately.

ICT Support department is responsible for ensuring that any security breach is dealt with within the shortest time possible to minimise disruption to institution operations.

Website Disruption

In the event that institution website is disrupted, the following actions must be immediately undertaken:

1. Website host to be notified
2. ICT Support department must be notified immediately
3. The main University administration team must be notified

Exemptions

This policy is mandatory unless Bugema University administration grants an exemption. Any requests for exemptions from any of these directives, should be referred to the Bugema University administration.

Breach of this policy

Any breach of this policy will be referred to Human resource manager who will review the breach and determine adequate consequences, which can include confiscation of the device and or termination of employment.

Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify ICT Support department immediately. In the event that the breach is not reported and it is determined that an employee failed to report the breach, then that employee will be referred to Human resource department for further consultation.

Indemnity

Bugema University bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of staff in accessing or using these resources or facilities. All staff indemnify Bugema University against any and all damages, costs and expenses suffered by Bugema University arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement. Legal prosecution following a breach of these conditions may result independently from any action by Bugema University.

References

- University of Huddersfield
https://www.hud.ac.uk/media/policydocuments/IT-Security-Policy.pdf

-The **Finchglow Group** IT Policy and Procedure Manual -01/08/2018

https://www.academia.edu/40152727/Information_Technology_Policy_and_Procedure_Manual

-The Uganda data protection and privacy act, 2019

- Blended Learning Policy For Bugema University.

-https://www.michigan.gov/documents/msp/Password_policy_325048_7.pdf

Bugema University ICT Support Policy Administration

		Signatures
Approval Authority	BU Administration	
Approval date		
Implementation date	August 2020	
Date of review	July 2021	
Author	ICT Support Department	