



Information & Communications Technology Policy

19th July, 2019

INFORMATION TECHNOLOGY SERVICES DEPARTMENT

DOCUMENT CONTROL INFORMATION	
Document Name	ICT Policy
Document Control Number	ICT0100
Approved / Endorsed by	Manager ICT / IBSUniversity Council
Approval / Endorsement date	19 th July, 2019 / 16 th August, 2019
Version	1.1
Review date	March 29, 2019
Author	Manager ICT
Owner	Manager ICT
Network Storage	Staff Common Folder

REVIEW HISTORY				
Version	Description	Date	Author	Owner
1	New policy	28.11.2018	ICT Manager	ICT Manager
1.1	Policy Review	29.03.2019	ICT Team Leader	ICT Manager




Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	<i>Page 2 of 34</i>

TABLE OF CONTENTS

S. No.		Page No.
PART 1: POLICY PREAMBLES		5-6
1	INTRODUCTION	5
2	PURPOSE	5
3	OBJECTIVES	5
4	SCOPE	6
5	DEFINITIONS	6
6.	ROLES & RESPONSIBILITIES	6
PART 2: POLICY GUIDELINES, PROCESSES AND PROCEDURES		7-23
7.	INFORMATION TECHNOLOGY USAGE	7-12
	Security of Information	7
	User Accounts	7-8
	Electronic Mail Usage (E-mail)	8-10
	Internet Usage	10-11
	Work Files	11
	Usage of Storage Devices (Portable/Permanent)	11
	Personal Files	11
	Violation	11
	Software	11-12
8.	MANAGEMENT OF INFORMATION TECHNOLOGY	11-17
	Information Technology Infrastructure Design	12-13
	Hardware and Software	13
	ICT Administration	13
	Application Licensing	13
	Virus Protection	13-14
	Electronic Mail	14
	Internet Access	14
	Internet Presence	14
	Physical and Environmental Security	14

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	<i>Page 3 of 34</i>

S. No.	Page No.
Network Security	15
User Account Policies and Management	15-16
Intranet Portal	16
Compliance	16
Business Continuity / Disaster Recovery	16
Incident Response	17
9. SERVICE LAPTOPS AND DESKTOPS	17
Laptop Security Risks	17
Compliance	17
10. PRINT COPIER USAGE	18-19
The Basics of Printer-Copier	18
Responsibilities	18
Abuse of Copier-Print Usage	19
11. IBSUNIVERSITY BACKUP RECOVERY	19-23
Responsibility	19
Backup Schedules	19-20
Backup Storage	21
Monthly Backups	21
Review or Testing of Backup Tapes	21
Data Backed Up	21
Archives	22
Restoration	22
Backup Storage Locations	22
 PART 3. FORMS AND APPENDICES	 22-34
Forms	22
Appendix 1: IT Email Sub-Policy	23-27
Appendix 2. IT System Asset Management Sub-Policy	27-28
Appendix 3. Computer Use & Internet Policy	28-34

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	<i>Page 4 of 34</i>

PART 1: POLICY PREAMBLES

1. INTRODUCTION

The IBSUniversity's Information & Communication Technology Department exists to support and enhance the IBSUniversity core mission of providing excellence in Education and Training for the staff, faculty, students and employees of corporate clients through the effective management and use of Information & Communication Technology resources.

The ICT Department does this through:

- 1.1 Providing appropriate access to information technology resources whenever possible for all students, faculty and staff.
- 1.2 Maintaining a stable and secure technology infrastructure implementing the appropriate security and risk management measures that can ensure availability, confidentiality and integrity.
- 1.3 Providing the collaboration tools that can enhance teaching and learning practices.
- 1.4 Providing timely, responsive and quality customer service to all students, faculty and staff of IBSUniversity through our service desk.
- 1.5 Implementing innovative ICT projects.
- 1.6 Fostering learning and growth for all ICT staff.


2. PURPOSE

To be a customer focused, cost-effective and well-run ICT Department that can be recognized for its responsiveness, flexibility and the effectiveness of the solutions it provides and supports.

Information & Communication Technology (ICT) Department exists to ensure the ICT needs of IBSUniversity is being met

3. OBJECTIVES

- 3.1 To support and enhance IBSUniversity core missions of education, training and research through the effective management and use of information technology resources and protection of data.
- 3.2 To evaluate, propose and deliver quality, timely and cost-effective ICT solutions and services to the alumni, students and staff of IBSUniversity thereby enabling them to achieve their personal, educational and professional goals.

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	<i>Page 5 of 34</i>

4. SCOPE

All users in access of the IBSUniversity’s computers, data networks and resources or who has custody of IBSUniversity information shall be required to be subject to this policy through the Service Level Agreement (SLA) with the third party. Hereinafter, all information, resources, and entities will be referred to collectively as IBSUniversity.

The policy observes clearly the Cyber Crime Act and NICTA Act of PNG.

5. DEFINITIONS

“**Backup**” is defined as the saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

“**Disaster Recovery**” is defined as the saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.

“**Information Technology Usage**” is defined to mean the use of computer and network resources by employees, students, suppliers and consultants while engaged in business activities of the IBSUniversity.

“**Laptop computer**” is defined to mean a small compact portable computer.

“**Management of Information Technology**” is defined to mean the managing, monitoring, and maintaining of IT standards, controls and procedures.

“**Print code**” is the code provided by ICT Department that allows access to copier/printer for print and copy.

“**Restore**” is defined as the process of bringing storage data back from the media and putting it on a storage system such as a file server.


“**User**” is a person that uses the facility provided.

6. ROLES & RESPONSIBILITIES

ICT Manager is responsible for ensuring that this policy is implemented fully to ensure that the ICT operations of IBS is operating effectively.

ICT Officers are responsible for complying with the policy clauses at all times in the process of executing their delegated responsibilities and tasks.

All staff of IBSUniversity are responsible for complying with the ICT policies on internet use, email use and laptop/desktop computers issued.

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 6 of 34

PART 2: POLICY GUIDELINES, PROCESSES AND PROCEDURES

7. INFORMATION TECHNOLOGY USAGE

7.1 Policy Guidelines

To ensure that:


- (a) Integrity of business information is preserved to support high quality services and effective decision making,
- (b) Confident and sensitive business information is protected,
- (c) There is clear accountability of the storage and usage of business information,
- (d) Promotion of user awareness and understanding of available information technology resources,
- (e) IBSUniversity legal options and employees' legal rights are preserved in the event of misuse or abuse of information resources.

7.2 Security of Information

- (a) If sensitive, confidential and/or private information is or is suspected to be lost or disclosed to unauthorised parties or unauthorised use of IBSUniversity information systems has taken place or is suspected to be IBSUniversity management should be notified immediately.
- (b) Employees or users of IBSUniversity information technology services shall not test security mechanisms at IBSUniversity facilities or use and /or possess tools for hacking and/or cracking information security.
- (c) IBSUniversity may keep logs on and reserves the right to examine:
 - i. electronic mail messages;
 - ii. files on computers;
 - iii. web-browser cache files;
 - iv. web-browser bookmarks and cookies;
 - v. logs of website visited and;
 - vi. other information stored on or passing through IBSUniversity computers, as and when it deems necessary.

7.3 User Accounts

- (a) All employees requiring access to internet, email, EMS or network services, will be provided with a unique User-ID.


Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	<i>Page 7 of 34</i>

- (b) User-IDs are not to be shared or used by employees other than the employee to whom the user-ID was assigned; users will be responsible for all actions taken with or against their User-ID.
- (c) Passwords, when required to be changed, will be sufficiently complex (avoid names, places, birthdays, company slogans, dictionary words etc.), so as to ensure that it cannot be figured out by other persons. Writing passwords down and leaving them where others could discover them is strictly prohibited.
- (d) Users shall leave a terminal/workstation or computer unattended if only it has an active logon session connected to it, with an auto-closed command after 10 minutes.
- (e) Least User Privilege to comply with information security policies must accompany all formal requests for authorization or reauthorization of a new use-ID and authorization of a change in privileges associated with an existing user-ID.
- (f) A user’s immediate manager is responsible for reporting changes in user duties that impact the need to access information or systems.
- (g) Users shall be responsible for all actions taken with their User-ID.
- (h) Passwords must be sufficiently complex (avoid names, places, birthdays, company slogans, dictionary words etc.), including a minimum password length of 7 characters, password changes at least every 90 days, contains both alphabetic and non-alphabetic characters, both upper and lowercase characters, password history of at least 1, and minimum password age of 2 days.

7.4 Electronic Mail Usage (E-mail)

A separate Information Technology Email Policy is attached as an appendix, *refer Appendix 1*, to this procedure. It further highlights in detail the expectations of the IT Email Policy.

- (a) IBSUniversity e-mail services will be used for business purposes only and as a productivity enhancement tool. Personal emails of any sort will not be sent or received using the company email assigned.
- (b) Incidental personal emails (those that are not related to the conducting of business on behalf of IBSUniversity), are not to be sent using IBSUniversity email system.
- (c) In no event shall any employee create or transmit e-mail messages that include offensive material that could be considered as harassing, discriminatory, defamatory, disruptive, illegal, or criminal, or that includes obscene, vulgar, or sexually explicit content.
- (d) Electronic mail systems and all messages, including back-up copies, are the property of IBSUniversity. IBSUniversity is committed to respecting the rights of its employees, including their reasonable expectation of privacy. However, users should be aware that IBSUniversity reserves the right, in case of incident report or


Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 8 of 34

employee is suspected of illegal use, to examine the content of electronic communications. Logging and monitoring may take place in order to support; operational, auditing, legal, ethical or investigative activities.

- (e) Users are prohibited from allowing anyone else to use their electronic mail account (including family, friends, and other users) and reading or attempting to read any other user's electronic communications (mail, calendars, folders), unless approved by management.
- (f) Users shall treat electronic mail as they would treat any other company communications; when an email is sent, the sender shall ensure that the proper etiquette for written communication is observed and that remarks that contain profanity, obscenities or derogatory remarks, even if made in jest, are excluded.
- (g) A legal recipient disclaimer will be added to all external electronic mail messages. This disclaimer will be as follows:

***DISCLAIMER:** This message is for the designated recipient only and may contain privileged or confidential information and exempt from disclosure under applicable law and/or may be subject to copyright protection. If you have received it in error, please notify the sender immediately and delete this message. Any other use of the email by you is strictly prohibited. Opinions, conclusions and other information in this message that do not relate to the official business of the organisation shall be understood as neither given nor endorsed by the organisation. The organisation makes no warranties that this message is free from malware and the like, and disclaims all liabilities in connection therewith.*

- (h) Users may not misrepresent or falsify their identity in any e-mail communications. The user name, organization and other company specific information shall be included in the message.
- (i) Users shall refrain from opening e-mail or attachments from which they do not know the sender or when the subject of the message seems inappropriate. Users shall not respond to an unknown sender under any circumstances.
- (j) Any e-mail containing a formal approval to conduct business, or constituting any commitment (financial or otherwise) by IBSUniversity to any outside organization must be approved by the Chairman or Vice Chancellor.
- (k) If unauthorized use of IBSUniversity e-mail systems has taken place or is suspected to have taken place, HR shall be notified immediately if involving staff and Pro Vice Chancellor if involving students to take appropriate actions.
- (l) Users are not authorized to join mailing groups, or any such form of distribution network that will lead to the receipt of non-business-related emails through your IBSUniversity email account.

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY Focusing on Student Centred Learning
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 9 of 34

- (m) Emails transmitted or received using the company email system belong to and remain property of the company; users are not permitted to delete, or modify correspondence when they leave and shall comply with HR exit policy.
- (n) HR to decide who is to email to all users/email group. Any email least privilege policy will be implemented upon HR Policy


7.5 Internet Usage

- (a) All employees that have access to the internet are expected to understand and comply with this policy. IBSUniversity's connection to the Internet can expose the company to many potential risks; to mitigate and address risks that are associated with Internet connection, these policies must be strictly followed.
- (b) Internet access will be provided to those employees that require it to conduct their duties. Access will be granted upon a request from an employee's manager.
- (c) Access to the Internet is provided to IBSUniversity employees to conduct business in an efficient and convenient manner. Incidental personal use is permissible so long as it does not: consume more than a trivial amount of resources; does not interfere with worker productivity; and does not pre-empt any business activity.
- (d) Personal accounts with online services (i.e. Kazaa, Skype or other services) that use their own software installed locally on a computer shall not be used or accessed from company computers.
- (e) Employees are strictly forbidden from visiting websites where content includes material that could be considered as offensive, harassing, discriminatory, defamatory, disruptive, illegal, or criminal, or that includes obscene, vulgar, or sexually explicit content.
- (f) No IBSUniversity servers shall be used to store or host personal web pages or web servers.
- (g) IBSUniversity will reserve the right to block access to internet sites deemed inappropriate. The ability to connect to a specific website does not in itself imply that employees are permitted to visit that site.
- (h) All non-standard software used to access the Internet must be approved by the ICT Manager and must incorporate all appropriate/approved vendor provided security patches.

All Web browsers should be configured to use regional connection or proxy standards.

ActiveX, Java, and JavaScript shall be restricted on un-trusted websites.

- (i) Access to internet services (i.e. web-based mail) from the Internet shall be via a secure (encrypted) login process. The use of fixed passwords over the Internet shall be prohibited as well as the saving of fixed password in the user's web browser.

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY Focusing on Student Centred Learning
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 10 of 34

- (j) The downloading of any software applications or software upgrades is strictly prohibited. Any and all requirements to download software should be referred to the ICT Manager.
- (k) Excessive use of social networking sites leads to cyber slacking because of excessive internet browsing, thus resulting in low productivity. As a result of that only certain hours every day are permitted for personal use in internet access. During this time access to personal email accounts, social networking sites, auction sites, etc. can be accessed.

7.6 Work Files

- (a) All documents/data created, updated and stored on workstations/servers by users are the property of the company.
- (b) Users who wish to copy data/documents must complete the relevant form, which must be signed by their manager and the ICT Manager.
- (c) Users must store their data in the “My Documents” folder. Under no circumstances are users permitted to store data elsewhere in the local drive.
- (d) Files are to be cleaned end of every academic year.

7.7 Use of Storage Devices (Portable/ Permanent)

- (a) The use of CD/DVD burner drives, flash drives and/or other storage devices is strictly prohibited, unless approved by management.
- (b) Personal Digital Assistant or PDA’s, mobile telephones or other digital devices that synchronise with Microsoft Outlook or other applications can only be used if approval is granted by Manager ICT.

7.8 Personal Files


Personal files or documents including music, personal photo galleries and video files are not to be stored on network or local drives.

7.9 Violation

Any employee who abuses the privilege of their access to e-mail/internet or network services or who is in violation of this policy will be subject to corrective action. Such corrective action may include: the removal of access to internet/email privileges; possible termination of employment, or; legal action. Refer HR Policy in respect to Email/Internet use violation.

7.10 Software

- (a) Unless authorised by ICT Manager in consultation with respective departmental manager or Head of School, under no circumstances are users permitted to install software on company computers.

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page II of 34

- (b) Users will be provided with standard set of applications as prescribed by management, and installed by ICT personnel.
- (c) Additional software requests will have to be justified and approved by Manager ICT in consultation with respective departmental managers, if approved will be installed by ICT personnel.


8. MANAGEMENT OF INFORMATION TECHNOLOGY

8.1 Policy Guidelines

- (a) ICT Department shall manage, monitor, maintain and upgrade all information technology infrastructure and data resources using best and current IT industry practices.
- (b) To ensure that by doing so it will contribute to the realization of the following business and management objectives which includes:
 - i. assuring the continued availability of IBSUniversity information resources to support business activities;
 - ii. preserving the integrity of business information to support high quality services and effective decision making;
 - iii. preserving the confidentiality of sensitive information technology resources and data;
 - iv. establishing clear accountability for the management and use of IBSUniversity information technology resources;
 - v. assuring the implementation of reasonable, cost-effective, and consistent group information security controls and procedures throughout IBSUniversity and its information technology systems and networks;
 - vi. promoting user awareness and understanding of IBSUniversity information technology resources;
 - vii. preserving IBSUniversity legal options and employee legal rights in the event of misuse or abuse of University information technology resources.
- (c) A separate Information Technology Asset Management Policy is attached as an appendix to this procedure. It provides in details the expectations of the ICT Management Policy (Refer to Appendix 2).

8.2 Information Technology Infrastructure Design

- (a) An Information Technology Infrastructure Blueprint (hereinafter referred to as “the Blueprint”) will be created and maintained, and will form the framework around which the actual physical and virtual ICT infrastructure and data networks will be built. The Blueprint will address the following areas:

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 12 of 34

- i. Network design & layout
 - ii. Hardware specifications
 - iii. Software specifications
 - iv. Enterprise Management System specifications
 - v. Security
 - vi. Data backup
 - vii. Telephony specifications
- (b) The purpose of the Blueprint will be to realise the business and management objectives as detailed in this Policy.
- (c) The Blueprint will be approved by the Vice Chancellor through the recommendation of the ICT Consultant and reviewed on an annual basis.

8.3 Hardware & Software

All hardware and software will meet the specifications of the Blueprint and will be procured by the ICT Department. All supplied hardware/software will be delivered to and setup in accordance with the current IBSUniversity system configuration prior to delivery to the end user.

8.4 ICT Administration


- (a) A suitably qualified professional will be employed by IBSUniversity for the purpose of carrying out the technical requirements of this policy and providing managerial and administrative services to users and management throughout the business.
- (b) All changes to network settings, configuration or layout will only be effected with the full knowledge and agreement of the ICT Manager.

8.5 Application Licensing

IBSUniversity will strictly enforce and adhere to software license agreements; free or open sourced software is recommended when no available license.

8.6 Virus Protection

- (a) IBSUniversity shall protect all electronic information, networks and computers from viral attacks and malicious software by installing licensed anti-virus software application(s) throughout the business. Where possible, a corporate edition will be installed at server rather than client level.
- (b) Third party computers (belonging to consultants, suppliers etc.) that are connected to the IBSUniversity network will be scanned.
- (c) ICT Department ensures that the AV database and application is updated daily.

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 13 of 34

8.7 Electronic Mail

- (a) IBSUniversity will operate an electronic mail system for use by employees upon the request of respective managers. Such email system(s) will be provided for the sole purpose of improving business efficiencies.
- (b) The usage of electronic mail will be governed by Email Usage Policy. *Refer 7.4 above.*
- (c) An approved legal recipient Disclaimer will be used by all users for email messages sent. *Refer 7.4 above.*

8.8 Internet Access

- (a) ICT Depart will provide internet/network access upon the request of the respective team leader/manager. For students, access is provided upon presentation of COA whilst for employees upon the request of respective managers. Such access will be provided for the purpose of improving business efficiencies and conducting company business.
- (b) Access to the internet by users shall be governed by the Internet Usage Policy. *Refer 7.5 above.*
- (c) Access to the internet shall be controlled by a User ID.
- (d) Internet/Network access is automatically disabled when the employee cease employment.

8.9 Internet Presence


ICT Department will maintain a site with the domain <http://www.ibsuniversity.ac.pg> for the purpose of promoting the company and its services to the customer base and the wider business community. All uploads to the website are to be approved by ICT Manager.

8.10 Physical and Environmental Security

- (a) IBSUniversity will ensure that its information technology infrastructure is physically secured and environmentally friendly.
- (b) Access to all network hardware will be physically restricted. Visitors or other third parties requiring access to hardware or software owned and managed by IBSUniversity will be controlled.


8.11 Network Security

- (a) IBSUniversity's computer systems and network facilities will be operated and managed in an appropriate manner to ensure they are adequately protected, secured, and used for company approved purposes only.
- (b) An active directory log will be maintained of all user profiles, along with their access privileges.
- (c) Virus related risks are to be isolated as much as possible and removed at all costs.

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 14 of 34

8.12 User Account Policies and Management

- (a) A formal process for identifying, authenticating and authorizing all users of systems must be in place for all systems. The term user-ID, in this document, refers to the unique name that identifies a user to a computer system.
- (b) In order to identify, authenticate and authorize users on the network, IBSUniversity primarily uses passwords. Logon access to the IBSUniversity network for authorized users will be further controlled to ensure that authorized users do not inadvertently provide or enable unauthorized access to a computer system and/or data files.
- (c) User-IDs must uniquely identify a single user. It should not be shared or given to anyone.
- (e) Naming standards will support a single User-ID for all platforms (unless specific systems preclude this option). Exceptions will be documented.
- (f) User accounts and passwords will be distributed to employees in a secure manner.
- (g) Additional restrictions will be placed on non-employee usernames and passwords including but not limited to audit and account/password policies.
- (h) Administrators/Super-Users shall maintain two accounts as required by test configuration: one privileged for administrative functions and one normal end user account for day-to-day activities. Administrators should use different passwords on each of the accounts.
- (i) Users will be required to change their password upon initial use/receipt and upon password reset.
- (j) Administrator accounts will require password changes at least within every 45 days.
- (k) Anonymous User-Id will not be allowed except for some servers supporting the use of anonymous FTP.
- (l) The limit on consecutive unsuccessful access attempts will be limited to 3 within a 60-minute timeframe. Once locked out, only the administrator can unlock the account primarily for security purposes or reasons.
- (m) There shall be a formal user registration and de-registration process for access to all multiuser ICT services. A Registration Form **[ICT0001]** and De-Registration Form **[ICT0002]** form requiring a user's immediate manager's sign-off will form the basis of all formal requests for a new user-ID or change in user-ID. For business applications, user access and privileges must be approved by the involved information owner. User-Ids shall be suspended after a specific period of inactivity.

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 15 of 34

8.13 Intranet Portal

- (a) IBSUniversity will maintain an intranet portal which will serve as a general information and documentation source for all employees. This site will be the repository for such documentation and information as: policies; procedures; contact information; product information and other general usage information.
- (b) In addition, IBSUniversity will also maintain a separate portal for students which will serve as a platform for learning matter to be stored, and access securely, without compromising intellectual property of the company.

8.14 Compliance


- (a) The design, operation, use and management of information systems may be subject to statutory, regulatory and contractual security requirements. Advice on specific legal requirements should be sought from the organization’s legal advisers, or suitably qualified legal practitioners.
- (b) Reviews should be performed against the appropriate security policies and the technical platforms and information systems should be audited for compliance with security implementation standards.

8.15 Business Continuity / Disaster Recovery

- (a) A Business Continuity Management Plan should be implemented to reduce any disruption caused by disasters and security failures as a result of natural disasters, accidents, equipment failures, and deliberate actions, to an acceptable level through a combination of preventative controls followed by backup alternatives in worse case scenarios.
- (b) The consequences of disasters, security failures and loss of service should be analysed and documented.
- (c) Contingency plans should be developed and implemented to ensure that essential business processes can be restored within the required time-scales. Such plans should be maintained and practised to become an integral part of all other management processes.
- (d) IBSUniversity’s will be protected by a reliable Uninterrupted Power Supply (UPS) system.

8.16 Incident Response

Refer to disaster risk management plan in order for timely respond to real or apparent security incidents to minimize damage, preserve evidence, and ensure response and resolution in compliance with relevant laws, regulations and IBSUniversity policies.

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 16 of 34

9. SERVICE LAPTOPS AND DESKTOPS

9.1 Policy Guidelines

- (a) All IBSUniversity employees issued with Laptop and Desktop computers shall strictly adhere to the guidelines outlined in this policy to prevent any loss, theft or misuse of the company property. The users will be held responsible for any loss, theft or misuse of the laptop/desktop computers.
- (b) Purpose:
- i. To ensure that the person allocated a laptop assumes an appropriate level of responsibility for IBSUniversity property.
 - ii. To ensure laptops are maintained in a secure environment to minimise the threat of loss or theft of the equipment itself and any sensitive information it may contain.

9.2 Security Risks of Laptop

- (a) Theft and Loss - Employees, IBSUniversity advisors and consultants and any one that IBSUniversity has authorised to be users of laptops shall take full responsibility for its safe keeping.
- (b) To counter the risks of theft and loss of laptop security must be addressed in the following ways;

It is the user's responsibility to:

- i. Have an increased awareness of the risks and to take precautions to keep the laptop safe and secure.
- ii. Be conscious of physical security; both at the user's home and when travelling
- iii. Be able to access control/ authentication on the laptop;
- iv. Enable data protection; using software and hardware-based solutions


9.3 Compliance

If in breach of any of the prescribed policies be responsible in notifying helpdesk immediately to assess the situation.

10. PRINT- COPIER USAGE

10.1 Policy Guidelines

- (a) All employees or suppliers and/or consultants that have access to photocopying, printing and scanning facilities of IBSUniversity must adhere to the procedures on proper usage of these resources.

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 17 of 34

- (b) Implementation of this policy will help achieve the following objectives:
- i. Management of weekly copier, printer limits
 - ii. Control and management of Print-Copy facilities
 - iii. Responsible use of print-copy facilities

10.2 The Basics of Printer-Copier

- (a) The copier and printers shall be used for company use only. There shall be no printing, copying and scanning of any personal information.
- (b) All users shall access printing and copying using an assigned access code.
- (c) All users with an access code shall be allocated a credit limit per week, (that is from Monday to Friday and the count will reset every Saturday by 1300 hours (though the weekly limit may be appealed).

Note: A double sided print/copy is counted as (2) copies or prints.

- (d) Print-Copy usage shall be actively monitored by the ICT Department.
- (e) When users' limits are reached, copying and printing will be prohibited further and shall only be permitted to continue under an appeal process as charged on a case by case basis.

Appeals may be subjected prior to the limits being reached but treated on a case by case basis. All bulk printing and copying are to be carried out by Logistic Department. A user can appeal once per week only and all appeals are to be approved by the respective team leader before submitting to IT.

10.3 Responsibilities


It is the user responsibility to ensure that the following guidelines are strictly adhered to when using the copier/printer.

- (a) No old crumpled papers are fed in the paper trays
- (b) Staples are removed before the papers are placed in the Automatic Document Feeder
- (c) Any fault in copier is logged immediately to IT Helpdesk
- (d) Daily Maximum for Copier/Printer is not exceeded

10.4 Abuse of Copier-Print Usage

Copier-Print Usage shall be strictly monitored and any abuse can result in the following penalties.

- (a) A user caught doing personal printing will pay for the total cost of the prints or copies
- (b) A user found to have caused damage to the copier due to negligence shall be dealt with accordingly by HR Department.

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 18 of 34

11. IBSUNIVERSITY BACKUP RECOVERY

11.1 Policy Guidelines

- (a) All servers, communication equipment and its configuration and critical data/applications owned and operated by IBSUniversity must be backed-up regularly for the purpose of disaster recovery and business continuity.
- (b) This policy defines the procedures to backup IBSUniversity critical data/applications and to provide the steps to recover data in the case of data loss due to human or natural disasters.

11.2 Responsibility


The ICT Manager/Team Leader shall delegate a Network Officer for each site to perform regular backups. The delegated person shall develop a procedure for testing backups and test the ability to restore data from backups randomly on a weekly basis and monthly on all the backups.

11.3 Backup Schedules

Full backups are performed nightly on Monday, Tuesday, Wednesday, Thursday, and Friday. If for maintenance reasons, backups are not performed on Friday, they shall be done on Saturday/Sunday. Backups are done by the Network officers of each site.

Systems will be backed-up according to the schedule below:

- (a) Data stored on the Student Management System live will be regularly backed-up as follows:
 - i. Full back up daily (Mon-Fri.) and data located on site.
 - ii. Full back up weekly (Sat.) and data located off-site.
- (b) Data stored on Student Management System will be regularly backed up as follows:
 - i. Full back up daily (Mon- Fri.) and data located on site.
 - ii. Full back up weekly (Sat.) and data located off-site.
- (c) Exchange Mailbox stores will be regularly backed up as follows:
 - i. Full back up daily (Mon-Fri.) and data located on site.
 - ii. Full back up weekly (Sat.) and data located off-site

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 19 of 34

- (d) Windows Servers (not in DMZ) will regularly be backed up as follows:
 - i. Incremental backup daily (Mon-Fri.) and data stored on-site.
 - ii. Full back up weekly (Sat.) and data located off-site.
- (e) The Virtual Machine Servers will have the Virtual Machine data drive regularly backed up as follows:
 - i. Image backup of virtual machines will be taken on Tuesday and Thursday. These backup files will be stored on-site
 - ii. Weekly file and folder full backup will be taken on Sunday. These backup files will be stored off-site.
- (f) Data Stored on user systems must be saved in My Documents Folder. This folder will be saved to the servers.
 - i. Back up of My Documents folder will be taken daily and stored onsite
 - ii. Back up of the documents folder will be taken weekly on Friday and stored offline.
 - iii. For staff that have left, a backup of copy of the user data will be archived in the Archive Folder 1 month after the user has left.
- (g) IOS images of routers and switches must be backed-up whenever a change is updated.


These images must be stored safely off-site.

11.4 Backup Storage

There shall be a separate or set of external hard drives for each backup day including Monday, Tuesday, Wednesday, and Thursday and Friday. There shall be a separate or set of flash drives for each Saturday of the month such as Saturday1, Saturday2, etc. Backups performed on weekends shall be kept for one month and used again the next month on the applicable Saturday. Backups performed Monday through Friday shall be kept for 3 weeks and used again after the 3 weeks has elapsed.

11.5 Monthly Backups

Every month a monthly backup external hard drive shall be made.


Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 20 of 34

11.6 Review or Testing of Backup Tapes

- (a) On a daily basis, logged information generated from each backup job will be reviewed for the following purposes:
 - i. To check for and correct errors
 - ii. To monitor the duration of the backup job.
 - iii. To optimize backup performance and take corrective action to reduce any risks associated with failed backups.
- (b) IT will identify problems and take corrective action to reduce any risks associated with failed backups.
- (c) Random Tests will be done once a week and at least monthly on all the backups in order to verify that backups are restorable.

11.7 Data Backed-Up

- (a) Data to be backed-up include the following information:
 - i. User data stored on the hard drive. (Users must save all critical business-related information in the “My documents” folder to be backed up).
 - ii. System state data
 - iii. The server registry
- (b) Systems to be backed-up include, but are not limited to:
 - i. File server
 - ii. Mail server
 - iii. Student Management System
 - iv. Domain controllers
 - v. Test database server
 - vi. My Document Folder
 - vii. Moodle
 - viii. Manage Engine

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 21 of 34

11.8 Archives

Archives are created at the end of every year in December. User account data associated with the file and mail servers are archived one month after they have left the organization.

11.9 Restoration

Users that need files restored must submit a request to the help desk. Include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

11.10 Backup Storage Locations


Appropriate Storage Device used for nightly backup shall be stored in an adjacent building in a fireproof safe. Monthly appropriate storage device shall be stored across off sites in a fireproof safe.

- (a) During transport or changes of drives, the appropriate storage device must not be left unattended.
- (b) The area where backups are stored must be secure and only accessible to ICT personnel only.
- (c) Weekly backups will be maintained for a period of 3 weeks.
- (d) After the period of 3 weeks has elapsed, the drives will be returned to ICT and will be either re-used or destroyed.
- (e) Media will be retired and disposed of as described below: Prior to retirement and disposal, IT will ensure that:
 - i. The flash drives no longer contain active backup images
 - ii. The media's current or former contents cannot be read or recovered by an unauthorized party.
 - iii. With all back up media, IT will ensure the physical destruction of media prior to disposal.

PART 3: FORMS AND APPENDICES

FORMS

<u>Code</u>	<u>Title</u>
ICT0001	Registration Form
ICT0002	Deregistration Approval Form

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 22 of 34


APPENDIX 1: IT EMAIL SUB-POLICY

1. Policy Guidelines

- (a) The purpose of this document is to streamline dissemination of information and management of activities through standardization of electronic mail composition format.
- (b) This policy applies to all employees and third-party consultants of the IBSUniversity of Business Studies (herein referred to as IBSUniversity), who are issued with IBSUniversity email addresses.
- (c) Objectives of this sub-policy is to;
 - i. Define use of the To, Cc, and Subject fields of an email.
 - ii. Define key words to be used in the Subject field.
 - iii. Define the response required by recipients of an email.
 - iv. Define the body/ content of email.
 - v. Define the use of attachments.
- (d) It is the responsibility of all employees to be familiar and practice use of these guidelines. Review and revision of this SOP is the responsibility of the IT Services Division as required.
- (e) Definitions
 - i. IT stands for Information Technology
 - ii. Email is Electronic-mail, sending of mail electronically
 - iv. IM stands for Instant messaging, instant sending of messages electronically
 - iv. CC stands for Carbon copy
 - v. BCC stands for Blind Carbon Copy
 - vi. Alias is a forwarding email address that does not actually exist as an account

2. Policy Process and Procedures


- (a) General
 - i. Where applicable, email correspondence should follow guidelines in preparing and managing correspondence.
 - ii. Employees should check their email at least twice per day (24-hour period).

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY Focusing on Student Centred Learning
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 23 of 34

- iii. Employees should minimize the number of non-work-related emails received via their IBSUniversity email account.
- iv. Employees should utilize the proper signature block format in closing. The signature block must include the current logo, along with your name, job title, and division and contact details.
- v. Employees who are not going to be available should notify their immediate Manager and utilize the “Vacation/ Out of Office” feature from the webmail system. The message should specify the duration of unavailability and alternate means of contact, as well as, a designated alternate contact during the period of absence.
- vi. Response timing is outlined in Section C. Keywords below.
- vii. Employees must ensure when replying that only relevant recipients are included in the To, Cc, and Bcc fields.
- viii. Employees are to refrain from replying to email alias such as “Staff All” and other lists unless there is a relevance to all users within that alias.
- ix. Employees must ensure that all emails sent must include the current disclaimer.

***DISCLAIMER:** This message is for the designated recipient only and may contain privileged or confidential information and exempt from disclosure under applicable law and/or may be subject to copyright protection. If you have received it in error, please notify the sender immediately and delete this message. Any other use of the email by you is strictly prohibited. Opinions, conclusions and other information in this message that do not relate to the official business of the IBSUniversity shall be understood as neither given nor endorsed by the organisation. The IBSUniversity makes no warranties that this message is free from malware and the like, and disclaims all liabilities in connection therewith.*

- x. Employees must not write emails in capitals.
- xi. Employees must seek approval from their Managers concerning newsgroup subscriptions; any formal agreements must include notification to the IT Services Manager.
- xii. Employees must ensure that the Inbox is kept empty, and all read emails are categorised into folders and logically organised in an effective manner.
- xiii. Employees are prohibited from allowing anyone else access to their email account.
- xiv. Employees must notify their manager if, they suspect any unauthorised use of emails has taken place, immediately.
- xv. Employees must not forward chain emails.

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 24 of 34

- xvi. Employees must be aware that viewing of pornographic, or sending pornographic jokes or stories via email, is considered as sexual harassment and will be dealt with accordingly.
- xvii. Employees must be aware that any emails that discriminate against employees by virtue of any protected classification including race, gender, nationality, religion, and so forth will be dealt with accordingly.
- xviii. Employees must be aware that any communications sent via email or stored on the organisation's equipment is property of IBSUNIVERSITY.
- xix. Employees must ensure they have backups of their emails; no assumptions should be made with regards to the organisation's backup procedures.
- xx. Any email containing a formal approval to conduct business, or constituting any commitment by IBSUNIVERSITY to any outside organisation must be approved by the employees' manager and must be in compliance with governing policies.


(b) Use of fields

- i. TO: Field. Email address(es) should be placed in this field if the recipient(s) is (are) required to respond or take action as a result of this email or the information directly affects their operations.
- ii. CC: Field. Email address(es) should be placed in this field if the recipient(s) benefit from knowledge of this communication but are NOT required to respond or take action as a result of receipt of this email.
- iii. SUBJECT: Field. Sufficient information should be placed in this field to inform the recipient of the desired response. Key words, as defined below should be utilized in the proper sequence to allow ease of identification and processing.

(c) Keywords

These keywords are defined for use in the Subject field only. They assist in the processing of the message by organizing content and specifying response. Key words should be utilized in the order shown below.

- i. INFORMATION. Recipients of this message should process the information. No response is required.
- ii. IMPORTANT. Recipients of this message should process the information and analyse the impact on operations. The recipient should utilize this information in the conduct of operations but no reply response is required.
- iii. ACTION. Recipients of this message should process the information and take appropriate action. A response is required for this message and should be accomplished by the suspense date. Upon receipt of this message by a recipient in the „To:“ field, they are required to acknowledge receipt and

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY Focusing on Student Centred Learning
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 25 of 34

ability to comply. Completed responses to this keyword shall be required in no less than 7 days. The sender should utilize the „read receipt“ feature of email applications. Should no acknowledgement response be received within one day, the sender should contact recipients in the „To:“ field via alternative means.

- iv. URGENT. Recipients of this message should process the information as quickly as possible and take appropriate action. A response is required for this message and should be accomplished by the suspense date. Upon receipt of this message by a recipient in the „To: “field, they are required to acknowledge receipt and ability to comply. Complete responses to this email shall be required in less than 3 days. The sender should utilize the „read receipt feature of email applications. Sender should also follow-up message telephonically as soon as practical after sending the message however no later than 24 hours.


For example: Subject: IMPORTANT: File server restart – scheduled

(d) Email Body

- i. Employees must ensure before sending emails that it is spelling and grammar error free.
- ii. IBSUNIVERSITY“s email style is informal. This means that sentences can be short and to the point. You can start your email with “Hi”, “Dear”, “Morning”, and the name of the person.
- iii. Employees can use IM acronyms such is COB (Close of Business), ASAP (As Soon As Possible), if they are positive that the reader will be able to fully understand what they are communicating, no assumptions must be made.
- iv. Messages can be ended with “Best Regards”, “Kind Regards”, and “Sincerely”.
- v. The use of characters such as smileys (-) is not permitted at all.

(e) Attachments

- i. Employees must ensure that attachments are compressed using maximum compression before sending.
- ii. Employees must ensure that attachments are scanned by the corporate antivirus solution provided.
- iii. Employees are discouraged from sending attachment with single files exceeding 2MB, due to email attachment restrictions in place by most email servers.

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY Focusing on Student Centred Learning
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 26 of 34

APPENDIX 2: IT SYSTEM ASSET MANAGEMENT SUB-POLICY

1. Policy Statement

- (a) This policy is intended to guide the Asset owner, Asset Manager and the Senior Management of IBSUNIVERSITY on the procedures to register, maintain and control the life cycle of IT Assets.
- (b) Implementation of this policy will result in the realisation and contribution of the following objectives.
- i. Maintenance of an Accurate IT inventory
 - ii. Maintenance and control of Software Assets
 - iii. Maintenance and control of Hardware Assets
 - iv. Proper procedures to dispose of an IT Asset Register
- (c) Definitions;
- i. **An IT asset** is a software or Hardware asset exceeding the value of a thousand kina, which requires ongoing maintenance and support, or creates potential risk in terms of financial loss, data loss or exposure.
 - ii. **Asset Registration** is the stage in which the equipment is categorised as an asset and registered on the IT asset Register.
 - iii. **An Asset Disposal** involves the process of disposing off faulty assets or assets that have depreciated in value.
 - iv. **Asset Relocation** is the transfer of Asset owner from one department or person to another.


2. Policy Process and Procedures

(a) Hardware Asset Control

Any equipment purchased valuing over a thousand kina which requires ongoing maintenance and support, or creates potential risk in terms of financial loss, data loss or exposure must be registered and controlled by the IT Asset Manager.

(b) Software Asset Control

Any software purchased by the company should be registered on the software Asset register. The Asset Register should maintain a complete license software Asset inventory that can provide a tool to assess compliance with the license agreements and whether the resources are being used efficiently and effectively. The information contained in this inventory should include product information, the business functions of the software, the users of the software and the cost associated with the license.

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 27 of 34

(c) Asset Disposal

The complete Asset Disposal process involves the following:

- i. Asset Disposal Form completed by Asset Manager
- ii. Asset Disposal Form approved by the director/chairman
- iii. Disposal of Items

(d) Asset Relocation or Transfer

The complete Asset Relocation process involves the following:

- i. Asset Return Form completed by current user. Before the form is signed the asset should be visually inspected to ensure that no damage has been incurred
- ii. Asset Manager relocates the asset to the new location and owner via the Asset Register
- iii. Usage policy signed by the new owner to show acceptance of usage policy

(e) Proper care

Proper use and care should be taken when handing or using Assets. In the case where an asset is found to be faulty due to negligence, penalties will be applied as this will breach the Asset Usage policy.

(f) Responsibilities

- i. It is the Asset Managers duty to:
 - ensure that the Asset Register is well maintained
 - enforce IT Asset Usage Policy (Laptop, Printer, Computer etc.)
- ii. It is the Users responsibility to:
 - ensure that the asset is well maintained


APPENDIX 3: COMPUTER USE AND INTERNET POLICY

1. Policy Guidelines

(a) Definitions

i. Computers

The term “Computers” means computer systems, operating systems, software or hardware purchased by and for the IBSUniversity, and includes peripherals equipment such as printers and scanners.

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 28 of 34

ii. Network Resources

The term “network resources” means Local Area Networks, other computerised networks or software, the Internet or world-wide web, websites, web hosting and on-line information services.

iii. E-mail

The term “e-mail” means electronic mail or electronic communication software systems.

(b) Purpose

This policy sets standards and restrictions for the use of the IBSUniversity computers, network resources, and e-mail in order to maintain cost efficiency, increase employee productivity, and reduce potential liability and inappropriate use. This policy shall be known as the Computer Use and Internet Policy.

2. Policy Process and Procedures

(a) Computer Use

i. Computer Use for Official Business Only


The use of the IBSUNIVERSITY automation systems, including computers, fax machines, and all forms of Internet access are intended for the official business purposes of the IBSUniversity. Managers shall determine and justify the extent of the availability to staff of computers, network resources and email. Those purposes include:

- Improving communications and information exchange within the IBSUniversity, and to entities outside of the IBSUniversity such as local and government agencies, relevant private sector companies; and
- provide access to information and research resources to staff and employees for the business of the IBSUniversity.

ii. Personal Use is Limited

Except as permitted in this policy, the IBSUniversity’s computers, network resources and e-mail are not to be used for entertainment, personal communications, other personal use, or illegal, harassing libelous or obscene purposes during or outside IBSUniversity business hours. In addition, staff and employees shall not connect their personal computers or laptops to the IBSUniversity’s internet access points.

Permitted personal uses are described in section 5.0 of this Policy. Personal use is a privilege and shall not interfere with official business or involve any expense to the IBSUniversity. This privilege may be revoked or limited at any time by the Chairman, Executive Director or the IT Administrator. The policy for personal use may be applied to Contractor personnel, External

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 29 of 34

Consultants, advisors, auditors and any other business visitors to the IBSUniversity.

(iii) Access to Network Resources Only On IBSUniversity Servers

Any and all business of the IBSUniversity conducted by the computer or through network resources of any kind shall be on secure servers hosted and managed by the IT Section under the management of the IBSUniversity's Chairman, Executive Director or his delegate.

(iv) Application of Policy

This Policy applies to all of the IBSUniversity's computers, network resources and e-mail and includes any information in digital electronic format such as e-mail, databases, clip art, digital images, voice and sound recordings or any other digitized information that may be available or developed and is stored on the IBSUniversity's computers.


(b) Inappropriate Use of Computers is Prohibited

IBSUniversity computers, network resources, and e-mail shall not be used inappropriately. Inappropriate use of such resources is cause for disciplinary actions in accordance with the IBSUniversity's Human Resources Policies manual. Criminal investigations by the PNG Police Force, or personnel investigation by any of the IBSUniversity's Divisions or the IT Administrator, of inappropriate use by any employee, do not constitute inappropriate use.

i. Definitions of Inappropriate Use

Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job activities. Use of the IBSUniversity's computers, networks and internet access is a privilege granted by management and may be revoked at any time for inappropriate conduct including, but not limited to:

- Seeking to gain or gaining unauthorised access to propriety information; or
- Hacking or otherwise seeking unauthorised access to passwords, computers or systems of the staff, individuals, businesses, Government Departments or the private sector companies; or
- Using or knowingly allowing another to use the internet for personal profit, personal business, commercial product advertisement or partisan political purposes not related to the IBSUniversity's official business; or
- Processing, distributing, transmitting, storing or displaying electronic material which is obscene, pornographic, profane, sexually explicit, libelous or defamatory; or

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 30 of 34

- Sending or posting confidential electronic material outside of the IBSUniversity or posting the IBSUniversity’s confidential electronic materials inside the IBSUniversity to unauthorised personnel; or
- Infringing on copyrights or other intellectual property rights, license agreements or other contracts (such as illegally manipulating, installing or making available copyrighted software, music or other protected intellectual property); or
- Forwarding unsolicited advertisements, junk mail or chain mail (also known as SPAM); or
- Accessing entertainment sites, such as games, movies, videos, chat rooms, music downloads; or
- Creating and distributing a computer virus; or
- Any other non-business use of a computer, network resource or e-mail;
- Misrepresenting oneself or the IBSUniversity;
- Engaging in unlawful or malicious activities;
- Using abusive, profane, threatening, racist, sexist or otherwise objectionable language in either public or private messages;
- Causing congestion, disruption, disablement, alteration or impairment of the IBSUniversity network systems;
- Defeating or attempting to defeat security restriction on the IBSUniversity systems and applications.

ii. Commercial Software

The IBSUniversity has licensed the use of certain commercial software application programs for business purposes. Third parties retain the ownership and distribution rights to such software. No staff member may create, use or distribute copies of such software that are not in compliance with the license agreements for the software.

(c) Permitted Personal Computer, Network Resource, and E-mail Use


The IBSUniversity automation systems are the IBSUniversity resources and re provided as business communication tools. Limited personal use of IBSUniversity computers, network resources, and e-mail is permitted, subject to the following limitations:

i. Limited Use

Brief and occasional personal use of the electronic mail system or the Internet is acceptable as long as it is not excessive or inappropriate, occurs before or after office hours or during authorised personal time (lunch breaks or other work breaks).

ii. No Cost

Personal use is permitted only for uses that do not create user charges to the IBSUniversity.

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY Focusing on Student Centred Learning
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 31 of 34

iii. Music

Streaming music is permitted as long as such use does not infringe on intellectual property rights or interfere with or interrupt others in an office.

(d) Rights to Inspect IBSUniversity Computers

IBSUniversity owns the rights to all data and files in any of its computers and Laptops, network, or other information systems used by the IBSUniversity.

i. The IBSUniversity reserves the right to:

- monitor computers and e-mail usage, both as it occurs and in the form of account histories and their content.
- inspect any and all files stored in any areas of the network or on any types of computer storage media in order to assure compliance with this policy and the relevant PNG Laws.
- comply with reasonable request from law enforcement and regulatory agencies for logs, diaries, archives or files on individual computer and e-mail activities.
- monitor electronic mail messages and their content. Staff must be aware that the electronic mail messages sent and received using the IBSUniversity equipment are not private and are subject to viewing, downloading, inspection, release, and archiving by the IBSUniversity Management at all times.

ii. No Staff may access another staff member’s computer, computer files or electronic mail messages without prior authorisation from either the staff member or an appropriate IBSUniversity Section Head.

(e) Computer Security Oversight, Investigations and Sanctions


i. Security Oversight

The IT Administrator, the Internal Auditor and other appropriate staff reserve the right to review employees’ use of computers, network resources or e-mail to determine whether such use is appropriate and conforms to this policy.

ii. Investigations

The IT Administrator is charged with the responsibility of conducting general investigations of the use of computers, network resources or e-mail by the IBSUniversity staff on his or her own or by request of the Section Head.

If the IT Administrator determines that a staff member has committed a prohibited or inappropriate use of computers, network resources or e-mail, the IT Administrator shall report such use to the appropriate authority, including the Chairman, Executive Director or the Criminal Investigation Division or the “Police Force.”

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY Focusing on Student Centred Learning
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 32 of 34

- It is a violation of IBSUniversity policy for any staff member, including the ICT Manager and Assistant, to access electronic mail and computers systems files to satisfy curiosity about the affairs of others. Staff found to have engaged in such activities will be subject to disciplinary action.
- IBSUniversity will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual Internet activities.

iii. Sanctions for Inappropriate Use of Computers, Network Resources, or E-mail

If a staff member is found by the IT Administrator to be violating the Computer Use and Internet Policy, the staff's access to the IBSUniversity's computers, network resources or e-mail may be revoked. In addition, appropriate disciplinary actions may be authorised in accordance with the HR Policies Manual, up to and including dismissal and criminal prosecution. Staffs are individually liable for any or all damages incurred as a result of violating IBSUniversity security, copyright and licensing agreements.

(f) Actions to Take


- i. If you have received any material which is obscene, pornographic, profane, sexually explicit, libelous or defamatory, immediately contact the IT Administrator to initiate an investigation and have such material deleted.
- ii. Staffs who inadvertently or unintentionally receives such material should delete it from their computer.

(g) Guidelines

The IT Administrator shall be responsible for establishing guidelines for use of computers, network resources and e-mail.

3. Laptop Users' Responsibility and Security Requirements


- (a) Laptop users must agree to take shared responsibility for the security of their laptop and the information it contains. Upon allocation of the laptop, the user must complete a "Laptop Custodian Agreement" and undertake to comply with all applicable sections of this Laptop Usage Policy.
- (b) Laptops issued to employees remain the property of the company. When the laptop is allocated to an individual, the user assumes temporary "custodianship" of the laptop.
- (c) Upon leaving IBSUniversity, the individual must return the laptop to the ICT Department, re-signing their original "Laptop Custodian Agreement". This releases the individual from their responsibility of the "custodianship" of the Laptop.

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY <small>Focusing on Student Centred Learning</small>
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 33 of 34

- (d) Users must take all reasonable steps to protect against the installation of unlicensed or malicious software. The use of unlicensed software (software piracy) is illegal and puts the organisation at significant risk of legal action.
- (e) Executable software must, whenever possible, be validated and approved by the ICT Manager before being installed into the IT environment. Unmanaged installations can compromise the IT operating environment and also constitute a security risk, including the intentional or unintentional spreading of software viruses and other malicious software.

Commercial software (including shareware) must:

- ii. Have a valid license for each prospective user
 - iii. Be checked for all known security risks, including malicious software.
- (f) Users must take good care of their laptop. Laptops are more fragile than desktops and require more care. The following recommendations on care and maintenance should be followed:
- i. Be careful not to bump or drop the laptop, do not carry items with it that could harm it and do not put any objects on top of it. The case, although strong, is not made to support extra weight.
 - ii. Take care when handling and storing the network connection cable. It can be damaged easily.
 - iii. When transporting the Laptop always turn it off and put it in a carrying case.
 - iv. Avoid touching the screen.
 - v. Avoid subjecting the laptop to extreme temperature changes. Components can become very brittle and easy to break, laptop is safest at temperatures that are comfortable for the user.
 - vi. Keep all liquids away from your laptop. Almost any liquid spill on the laptop can result in extremely expensive repairs.
 - vii. Keep memory sticks, computer drives and laptop away from magnetic fields. Magnetic fields can erase data on memory sticks and computer drives.
 - viii. Whenever possible, avoid turning off laptop when the hard drive light is on because data on the hard drive could be lost or corrupted.

Prepared by: ICT Manager	Reviewed by: Policy Review Committee	Approved by: Manager ICT	 IBSU UNIVERSITY Focusing on Student Centred Learning
Document Control No: ICT0100	Version No. 1.1	Approval date: 19.07.2019	Page 34 of 34