IT POLICY

Step towards drawing a suitable Information Technology (IT) policy for all IT data, equipment, services and processes in the domain of UoB DIT ownership and control.

PURPOSE OF POLICY

The purpose of this policy is to outline the acceptable use of information technology resources at University of Balochistan in order to:

- Comply with legal and contractual requirements;
- Protect the University against damaging legal consequences and;
- Safeguard these resources.

SCOPE OF POLICY

This policy is applicable across the University and individually applies to:

- All individuals who have access to University's information and technologies.
- External parties that provide information processing services to the University.

DEFINITIONS

Approvals

The formal endorsement of a document in the form of physical signature after a thorough review from relevant stakeholders.

Copyright

Exclusive rights to print and publish material.

Confidential Information

Privileged communication shared with only a few people for furthering certain purposes.

Form

A form is an informational document with spaces (fields) for input of relevant information for which the document is associated. A form, after it has been filled, maybe a statement, IT request or an order.

IT

Information Technology, the set of technologies that involve the development, maintenance, and use of computer systems, software, and networks for processing and distribution of data.

Cybercrime

Also called computer crime is the use of a computer connected over a network (wired or wireless) as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities and/or violating privacy.

DIT

Directorate of Information Technology, (A Directorate) in University of Balochistan, Quetta.

Application

Any software (in-house developed or outsource vendor product).

License

Authorize use for a certain purpose.

Policy

A document that defines the boundaries through which standard operating procedures can be developed and maintained.

Procedure

A document that defines detailed process-specific instructions on how to perform particular tasks or react in particular situations.

Guideline

A general statement(s) document that helps in determining the course of action.

Proprietary Data

Internally generated data or documents that contain technical or other types of information controlled by an organization to safeguard its competitive edge.

Responsibility

The liability and obligation of an employee in the IT department to carry out the implementation of process and adhere to relevant IT policy and procedure document(s).

Security

On a network, protection of a computer system and its data from any sort of harm or loss, implemented especially so that only authorized users can gain access to shared files/data.

VPN

A virtual private network (**VPN**) is a configuration that creates a safe and encrypted connection over a less secure network, such as the public Internet. A **VPN** works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols.

PABX

Private Automated Branch Exchange, this telephone network is commonly used by call centers and other organizations. PABX allows a single access number to offer multiple lines to outside callers while providing a range of external lines to internal callers or staff.

FTP

File Transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet over TCP/IP connections. Using FTP, a client can upload, download, delete, rename, move and copy files on a server.The functional areas that are broadly covered are described in following order;

INTERCOM FACILITY

Faculty members and other UoB personnel desiring intercom point should send a written request to Director DIT through their sectional/departmental head. Upon receipt of request, the Director would get a survey conducted and if feasible, the connection for intercom will be provided with subject to the availability of resources and slots in PABX. In case of financial implication beyond the available resources of DIT, it would be the responsibility of applicant's sectional/departmental head to get the funds approved or purchase the required equipment through purchase section of UoB.

The call received on DIT's main exchange room are transferred to relevant personnel by the operator.

CUSTOMIZED COMPUTER SOFTWARE APPLICATIONS DEVELOPMENT AND MAINTENANCE

1. Any request pertaining to the customized / specialized software should be sent to Director DIT, who will instruct the System Analyst to examine the need and provide his/her feedback. Upon the recommendations, the Director will constitute a technical team comprising of System Analyst, Programmer, Web Master, etc. to analyze the feasibility whether that particular software could be developed inhouse or in other case, the requirements will be floated to third parties including outside vendors, companies, etc. as per rules for the development of software if deemed essential and as per availability of the budget.
2. In case it is decided to develop the software inhouse, then it will be the responsibility of the UoB Programmers to develop the software as per requirements under the supervision of concerned System Analysts. Subsequently, that particular Software developer and its relevant team will be responsible to troubleshoot or maintain the software in future as well, while assuring the protection of software code and relevant data.

3. Under any scenario where a software loophole or breach has been found, the programmers will immediately take remedial measures for the protection of system.
4. Only relevant programmer and the development / maintenance team will have the direct access to the source code, database and the computer server where the software has been hosted or installed. In case of any software or its data rectification including the database table entry, the concerned personnel may forward a request duly endorsed by the sectional head to Director DIT.

All UoB customized software Application will remain the sole property of UoB with all exclusive rights. In case of any violation, copyright infringements, source code or data theft, unauthorized access to software and its data may lead towards legal actions under the prevailing Cyber Laws of the Government of Pakistan.

USER ACCOUNT REQUEST (WIFI, VPN, EMAIL, FTP)

1. Faculty members, students, officers and employees will request for creation of user credentials / accounts through designated forms duly endorsed by the HoD / sectional head to access UoB Smart University WiFi, VPN, Email, FTP facility etc. Subsequently, the user account will be created and maintained in their department organizational unit (OU) under the UoB domain. VPN enabled accounts can be used to access the digital library from outside the UoB network. Furthermore, the accounts of personnel can be officially used for emails. All the users are required to check their accounts for any possible mails at least once in every 48 hours, whereas, all sectional/departmental/faculty heads are required to check their e-mails at least once in every 24 hours.
2. User account holders will ensure protection of their credentials including the password, by not disclosing that to anyone else. In case of possible breach of credentials, the user must notify in written to Network Administrator DIT.
3. The Email users will ensure to regularly change their passwords.
4. FTP accounts can only be requested by personnel duly forward by HoD / Dean, who are maintaining their departmental / sectional website internally. It will be their responsibility to ensure the protection of data against any misuse, etc.
5. Users should save important emails from UoB mail server through outlook (POP3) as mails will be deleted on periodic basis from the UoB email server.

DIT SUPPORT / HELP DESK

DIT is responsible for monitoring all network facilities like Web, Email, LAN/WAN, WiFi, VPN and FTP, etc. Furthermore, DIT is also responsible for maintaining the IT infrastructure.

To facilitate the stake holders to IT related complaints, DIT maintains a support center / help desk, at Network Operations Center (NOC). DIT Technical Staff can be contacted on the following numbers:

- Telephone Contact: +92 81 9211008 (Intercom: 1111, 2001, 0)
- Email: dit@um.uob.edu.pk.

WEBSITE CONTENTS PUBLISHING

Information uploading on the UoB website would be through Director DIT. The Director DIT directs the webmaster to upload the desired content / information / document.

1. Information of all Exams and results of UoB must be published on the website.
2. All UoB advertisements sent for publishing in the newspapers must also be sent to the webmaster for web publishing.
3. Information about research journals will be sent to webmaster for publishing duly endorsed by HoD/ Sectional Head/ Dean.
4. All the material to be uploaded to the UoB website must be emailed on dit@um.uob.edu.pk and addressed to Director DIT at least 24 hours before it is to be posted on the website.
5. For removal of any content from UoB official website, a formal request processed through sectional head and duly endorsed by concerned Dean or Registrar may be sent to Director DIT. However, any outdated or other content that is no more needed will automatically be removed by the webmaster.
6. All website update requests will be served as soon as possible.
7. The data and information uploaded on the official website of UoB remains the sole property of UoB. Therefore, any unauthorized copying of data & information is strictly prohibited. Webmaster will examine and analyze the site traffic for this purpose.

8. The authenticity of the data of all departments published on website is the responsibility of the concerned department.
9. All the Deans /HoD /HR section to provide the details regarding their respective faculty in terms of any changes of departmental head, faculty qualification, retirement, study leave, etc. to the webmaster.

EMPLOYEE HOSTING PRIVATE WEBSITES

Employees are not allowed to create web pages or sites that reference UoB or affiliate, masquerade as UoB, or in any way disclose any other information about UoB without the written permission of the management. Employees are not allowed to host personal sites on UoB facilities.

INTRANET/ INTERNET/ VPN/ E-MAIL/ FTP USAGE

The UoB Intranet/ Internet/ VPN/ FTP and other IT services are for the benefit of all UoB stakeholders. Intranet/ Internet/ VPN/ FTP, however, are shared facilities and must be used properly. Choking of bandwidth by a single user can impact all other users who are using the same shared facility. Internet and email should not be used to access or disseminate illegal, defamatory, or potentially offensive information/content. Computer and network usage will be governed by the following policy:

1. Internet usage must be for Educational & Research purposes.
2. On one user account, only one machine should be connected via Access Point. However, with same credentials, the user can also connect his / her smart mobile phone or tablet as well.
3. Peer-to-Peer file sharing / Download software must not be downloaded and used.
4. Avoid sending and receiving any suspicious file. Furthermore, no illegal / material may either be accessed or sent while using the UoB network.
5. UoB Email should be checked frequently and should be used for official purposes only. No objectionable material must be transmitted using UoB network/email resources.
6. All UoB computer users must ensure the copyrights in the works that are accessible through UoB network. Furthermore, no copyrighted work may be copied, published, disseminated, displayed, performed, or played without permission of the copyright holder except in accordance with the fair use or licensed agreement.
7. DIT may require identity of machines (e.g. MAC / physical address) to allow or block access of machine to the Local Area Network. In case of violations of IT policy or improper use of LAN/WAN/WiFi, DIT may block any user/machine at any time without any prior notice.

NEW INTERNET CONNECTION REQUEST

Any request pertaining to a new internet connection may directly be sent to Director DIT, duly endorsed by the sectional head. Such requests will be forwarded to the concerned IT personnel for further necessary action. Incase, the connection cannot be provided due to lack of IT infrastructure especially, in any newly constructed building or vicinity, then alternatively, third party internet connectivity may be temporarily provided, until the deployment of proper IT infrastructure.

REMOTE ACCESS

Remote access policy applies to all UOB personnel and students connected to UoB Network via VPN, Remote Desktop or FTP etc.

1. Any remote access must be requested and duly endorsed by HoD / sectional head on prescribed form.
2. It is the responsibility of UOB personnel and students having remote access to UOB's network to ensure fair / legal usage for educational and research purpose.
3. UOB personnel is responsible to ensure that their family members do not violate any UOB policies and do not perform any illegal activities as well. UOB personnel bears responsibility for the consequences in case of misuse of granted access.
4. Secure remote access must be strictly controlled via password authentication.

5. UOB personnel should never provide their login or email password to anyone, not even to any of their family members.
6. UOB personnel and students with remote access to UOB organizational network must not use non-UOB email accounts (i.e., Hotmail, Yahoo, Gmail) or other external resources to conduct UOB official correspondences.
7. All those nodes that are connected to UOB internal networks via remote access technologies must use the most up-to-date antivirus software.
8. Any issues pertaining to remote access must be communicated to Network Administrator DIT.

VIDEO CONFERENCING

Video Conferencing facility intends to provide an interactive live platform for communication and is based on hardware and software-based solutions. This facility can be accessed and used:

1. With an official request forwarded by HoD / Dean, for utilizing the facility at video conference hall or other designated locations.
2. The contents delivered via video conferencing should be acceptable, permissible, and legal that are related to education and research purposes only or official meetings.
3. Anyone using Skype, WhatsApp or other social media-based audio / video software programs / Apps via UoB Network will be responsible for the content that they receive or deliver. The usage must be ethical and related to education and research purposes only.

SECURITY AND USE OF E-RESOURCES

The adhering of appropriate measures for being free from unacceptable risk is the key concept behind security. The risk concerns the following categories of losses:

1. Information Confidentiality
2. Data Integrity
3. IT Assets
4. Efficient and appropriate acceptable Use.
5. Network / System Availability.

The assets that must be protected include:

1. Computer & related Equipment
2. Telephony Equipment including PABX.
3. Computing & Communications Sites
4. Data Storage Media & Related Equipment
5. Computer Software (System / Application) Programs & Documentation
6. Data & Information including databases.

GENERAL USE AND OWNERSHIP

1. While UOB IT administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the organizational systems remains the property of UOB.
2. Any unauthorized copying of UoB Data / Information will be termed as information theft.
3. Personnel are responsible for exercising good judgment regarding the rationality of computer use.
4. Personal use of Internet/Intranet/VPN/PABX systems, is discouraged, expect for the purpose of educational research.
5. For security and network maintenance purposes, authorized individuals of DIT within UOB may monitor equipment, systems and network traffic at any time.
6. DIT UOB reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
7. The Pakistan Educational Research Network (PERN) fair usage policy will also be part and parcel of this policy document.

SECURITY AND PROPRIETARY INFORMATION

1. It is the responsibility of the official to protect and safeguard any equipment installed at the premises / vicinity of his/ her use or control. However, any loss or theft of IT equipment must be immediately reported to the higher authorities.

2. Password is a unique entity-key of an individual user to access UOB computing resources such as VPN, WiFi, Email, FTP etc. It must not be disclosed to others.
3. If a user forgets his / her password, then he/she must contact the network administrator with the password reset request. A user cannot ask network administrator to reset password of any other user. Network administrator may ask for any proof pertaining to the ownership of the account that may include ID / Official/student card.
4. Users are not allowed to Login on any other user's computer without their permission.
5. Users must protect their computers and the UOB network from computer viruses/malware, etc. All computer users must ensure that antivirus software is installed on their computer and that virus protection and firewall is enabled. No user should disable virus protection nor must antivirus software be prevented from scanning system files. All media, email, and internet downloads must be scanned for viruses.
6. Emails from unknown users must not be opened.
7. Users must report any suspicion of virus attacks immediately to DIT-NOC.
8. It is the responsibility of each computer user to protect all sensitive information of UOB. Users must refrain from unnecessary sharing of files and folders as this may put sensitive data at risk.
9. Users may not test or implement any products known to compromise the confidentiality, availability or integrity of UOB resources, data and information. It is illegal to possess, distribute, use or reproduce programs for scanning networks (such as tools used as packet sniffers, hacking, key logger, etc).
10. The user interface for information contained on Internet/Intranet systems should be classified as either confidential or not confidential. Examples of confidential information include but are not limited to: examinations material (e.g. question papers, award lists, etc.) university private, organizational strategies, competitor sensitive, trade secrets, specifications, lists, and research data. UoB personnel should take all necessary steps to prevent unauthorized access to this information.
11. All hosts used by the employee that are connected to the UOB Internet/Intranet, whether owned by the employee or UOB, shall continually be executing approved and updated virus-scanning.
12. Personnel must use extreme cautions while opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
13. All stakeholders using UoB Network (LAN/WAN/WiFi/VPN/FTP etc) must ensure utmost vigilance while accessing and clicking on unknown sites and weblinks.
14. Usage of UoB logo or internal materials in any web page or Internet posting is strictly prohibited unless it has been approved by the management.

UNACCEPTABLE USE

The following activities are, in general, prohibited.

Under no circumstances is an employee of UOB authorized to engage in any activity that is illegal under local, provincial, federal or international law while utilizing UOB-owned IT resources. The lists below are by no means exhaustive but are an attempt to provide a framework for activities which fall in the category of prohibited.

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for the use by UOB.
- Introduction of malicious programs into the network or its devices like servers (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a UOB computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any UOB account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to

access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

- Port scanning or security scanning is expressly prohibited.
- Use or possess Internet scanning or security vulnerability assessment tools, such as SATAN, ISS, NESSUS or NMAP.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Unauthorized copy and reproduction of information / data by any UoB personnel or third party from UoB Web or other online services will be considered as illegitimate unless used for official business of UoB.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet is strictly prohibited.
- Providing information about, or lists of UOB employees to outside UOB unless directed by UOB own policies.
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- UoB Network (LAN/WAN/WiFi/VPN/FTP etc) must not be used & accessed for personal use and to propagate false / illegal information, data, content via email or social media (WhatsApp, Twitter, Facebook etc)
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Any violation of UoB Internet policy can lead to disciplinary actions.
- University reserves the right to refer any case pertaining to cybercrime to the relevant authorities of Government of Pakistan.

In case of any point of importance missing in this policy, is deemed to be considered automatically embedded in this policy document, as per HEC’s / Government of Pakistan’s IT Policies.