INFORMATION TECHNOLOGY POLICY

Fakir Mohan University,
Vyasa Vihar,
Balasore-756089, Odisha.

1. Vision

To develop a robust IT infrastructure in the University Campus for transforming non-IT driven teaching-learning system to IT driven teaching-learning system and to promote IT driven administration with an emphasis on protection of data and information of the University.

2. Background

Fakir Mohan University named after Vyasa Kabi Fakir Mohan Senapati is the highest centre of learning for the districts of Balasore and Bhadrak. The University recognizes the vital role IT plays in the University's vision and missions and related administrative activities as well as the importance in an academic environment of protecting data and information.

Increasing usage of digital platform by students, faculty, and staff of the University creates more opportunities to use advanced technology to give utmost protection to data and information. This policy establishes University-wide strategies and responsibilities for computing facilities and protecting the Confidentiality, Reliability, Integrity, and Availability (CRIA) of the information assets that are accessed, created, managed, and/or controlled by the University.

This policy lays down general guidelines for the use of IT infrastructure of Fakir Mohan University. It is difficult to enumerate all but it is to be noted here that any activity which inconveniences users, depletes the IT resources of the University in general or jeopardizes the privacy and security of the systems, or violates IPR of software, amounts to unethical use.

3. Focus Areas

The focus areas of IT policy include: i) Departmental ICT facilities, ii)Procurement of ICT resources, iii) Maintenance of ICT resources, iv) Green ICT practices, and v) Privacy and Security.

3.1 Departmental ICT facilities

The individual departments shall be allowed to set-up computing laboratories/ICT facilities for high quality teaching and research. Permission for setting-up of such a facility shall be given by the Vice Chancellor on recommendation by the Teachers' Council of the Department with proper justification. Such specialized Labs/facilities may be funded by funding agencies through research projects or funded by University through developmental grant or through code money of the concerned Department. Such Labs/facilites will be maintained either by technical staff of the department/central computing facility center or by personnel employed under the concerned projects. On receiving requisition from the Department, the central computing facility centre (CCFC) shall take due steps to procure computing/ICT resources for the respective Department. If at any time a department is not in a position to continue maintenance of such resources, it may offer these to the CCFC to be included in the common resource pool of computing resources of the University. The department may consult the CCFC regarding the requirements for maintenance of the computing/ICT resources obtained through research

projects at the proposal preparation stage. The maintenance of computing/ICT resources under research projects shall be done under the respective project or by the concerned departments.

3.2 Procurement of ICT resources

The computing/ICT resources may be procured either by the University against the indent order placed by the CCFC or by the individual departments for their own laboratories/facilities. The process of procurement of the computing resources shall be as per the prevailing government rules and regulations. The specifications for the computing/ICT resources for the specialized laboratories of the individual departments shall be worked out by the respective departments and procurements will be as per existing government rules and regulations. Further, for procurement of any ICT resources always there must be two bids (technical and financial). If technical bid is satisfactory then only financial bid will be opened and comparative to be done. Also, if purchased through GeM, the technical specification shall be certified by the purchase committee.

3.3 Maintenance of ICT resources

The post-warranty maintenance of the Servers and the UPSs shall be carried out through AMC. The PCs and Laptops in the Central Computing facility Centre and those provided to the departments/sections through CCFC shall be maintained by the Technical Staff of the CCFC. Appropriate stock of spares shall be maintained for that purpose. The maintenance of the peripheral devices including teaching aids like LCD/LED projectors/CCTVs will be done through AMC, third party or by the skilled staff of CCFC/staff deployed in different Departments depending upon the cost and critical nature of the device. A small buffer of PCs, UPSs, and Printers shall be maintained for temporary replacement in critical usage cases.

3.4 Green ICT Practices

Due to growing concern in environmental responsibility, the computing/ICT resources should be used efficiently. The following green computing practices shall be adopted.

- Obsolete equipment disposal by following e-waste policy.
- Use of certified energy efficient and environment friendly equipment.
- Sharing printers, computing resources and storage over network.
- Keeping monitors in sleep mode or turn off mode when not in use.
- Activating power management feature on computers and peripherals.
- Use of email for circulation of office documents and memos and e-office for logical file movement.
- Reduce paper waste by printing as little as possible.
- Use of double sided printing.
- Refilling toner cartridge wherever possible and buy back of batteries by authorized vendors.
- Shifting to cloud-based services whenever possible.

3.5 Privacy and Security

The University has adopted standard procedure towards privacy and security of ICT resources.

- On shared computer system [like servers, HPC systems etc.] every user is assigned an ID. Nobody else should use an ID without explicit permission from the owner.
- All files belong to somebody. They should be assumed to be private and confidential unless the owner has explicitly made them available to others.
- Messages sent to other users should always identify the sender.
- Network traffic both on Intranet/Internet is implicitly private.
- Records, including logs relating to the use of computing and information resources are confidential.
- Nobody should deliberately attempt to degrade or disrupt computing and communication systems performance or to interfere with the work of others. Any attempt to disrupt service of performance on systems on or off campus can result in the loss of network privileges and disciplinary action. The following items are all examples of denial of service attacks, but are not completely inclusive.
    - Mail bombing (sending thousands of mail messages to a group or individual.
    - Ping flooding (launching continuous ping requests at a specific machine
    - "Smurf attacks"
    - "SYN flooding"

- Loopholes in computer systems or knowledge of a special password should not be used to alter computer systems, obtain extra resources, or take resources from another person. [Reframing of Sentence required].

- Computing/ICT equipment owned by academic/administrative units or individuals should be used only with the owner's permission.

- University resources are provided for university purposes. Any use of computing/ICT for commercial purposes or personal financial gain must be authorized in advance. While the university makes computer/ICT resources available primarily to achieve its goals of high quality teaching and research, it realizes the need to encourage the personal use of computing for the convenience of the campus community. The extent to which these resources are used for personal reasons is limited to strictly non-profit-oriented tasks. Thus, it is reasonable to allow the use of computing resources for computer mail, document preparation or other activity that can facilitate convenience or enhance productivity. Any personal use of computing resources that produces individual financial gain is prohibited unless permission has been taken and an account has been issued which releases this restriction.

- It is unethical to make so excessive a use of system resources [on Servers, HPC systems, communication system, etc.] that other users cannot obtain access to these resources. Examples include excessive use of CPU time during a period of heavy use on a timesharing system, excessive use of disk space on a system that does not limit such utilization, and use of an excessive amount of network bandwidth in an environment of networked personal computers. A novice user might well be unaware that a particular type of action

constitutes“excessive use”; but once a system administrator makes him or her aware of the fact that such an action is unreasonable, that user is to be held responsible for any further such infringement.

- Computing, Communication, and other IT resources are University resources. Theft, mutilation, and abuse of these resources violate the nature and spirit of community and intellectual inquiry.
- Users are responsible for the security and integrity of their systems. In cases where a computer is “hacked into”, it is recommended that the system be either shut down or be removed from the university campus network as soon as possible in order to localize any potential damage and to stop the attack from spreading. In such cases, if the system administrator cannot be contacted in a reasonable time, concerned authority reserves the right to disable the network connection. Once the system manager is made aware of the situation and agrees to take reasonable steps to ensure that the machine is not compromised, network privileges may be restored.
- In cases where, despite the efforts of the system manager, the machine continues to pose a security concern, we reserve the right to require that the user switch to a single user OS before allowing the system back onto the campus network.
- In case where a user’s machines habitually cause problems, by action, as a “target” of incoming attacks, or because of a lack of responsible behavior on the owner’s part, Computing Centre may initiate action to permanently ban the user from having machines on the campus network.
- Anonymous Mailers: All electronic communications at Fakir Mohan University must accurately identify the sender. Anonymous and masquerading mail forwarders are explicitly prohibited by the IT policy.
- Copyright Material [Example Music/Movies Files]: It is a common misconception that the creation and subsequent distribution of music files is an acceptable activity. The distribution of copyright protected materials is illegal and is in direct violation of the Computing Code of Ethics. Movies which are protected by copyright law, and to which you do not have a license to distribute, should be treated with the same consideration as music files. Copyright material from any website using FMU resources is prohibited.
- Obscenity material should NEVER be digitally stored, manipulated nor shared.
- Software Piracy: Distributing licensed software is illegal and constitutes a violation of the Computing Code of Ethics.

4. Central Computing Facilities Centre

The officer-in-charge as well as System Manager of Central Computing facility centre is responsible to implement the IT policy as approved by Vice Chancellor of Fakir Mohan University time to time with a due ratification in the syndicate. The CCFC is responsible for maintenance of the university owned computer systems, peripherals, and other teaching aids that are either under warranty or annual maintenance contract. The CCFC is also responsible for maintenance and up-gradation of Fakir Mohan university website as per Policy. The CCFC may receive complaints from Departments or any administrative section, if any of the particular computer systems

are causing network related problems. The CCFC will be responsible only for solving the hardware related problems or OS or any other application software that were legally purchased by the university and was installed by the company.

The CCFC or its technical staff should not encourage installing any unauthorized software on the computer systems of the users. They should strictly refrain from obliging such requests. When the CCFC or authorized technical staff reformat the computer systems and re-install OS and other application software, care should be taken to give the same hostname, IP address, network Mask, gateway as it was having earlier. Further, after installing the OS all the patches/latest service pack should also be properly installed. In case of antivirus software, technical staff of CCFC should make sure that its latest engine and pattern files are also downloaded from the net.

5. Misuse and Degree of Punishment

5.1 Misuse:

Any usage which contravenes local, state and central government laws or violates norms of Fakir Mohan University usage will be treated as misuse. All listed actions and others which effectively amount to the same are considered to be misuse of Fakir Mohan University's computing and ICT facility.

1. Using the network to gain unauthorised access to any computer system.
2. Tapping phone or network transmissions (e.g., running network sniffers without authorisation).
3. Knowingly performing an act which will interfere with the normal operation of computers, terminals, peripherals or networks.
4. Knowingly running, installing and/or giving to another user a program intended to damage or place excessive load on a computer system, network device or network. This includes, but is not limited to, programs known as computer viruses, Trojan horses, and worms.
5. Attempting to circumvent data protection schemes or uncover security loopholes.
6. Masking the identity of an account or machine.
7. Releasing a virus, worm or other program that damages or otherwise harms a device, system or network
8. Using Fakir Mohan University's resources for unauthorised purposes (e.g. using personal computers connected to the campus network to set up web servers for commercial or illegal purposes).
9. Unauthorised access to data or files even if they are not securely protected (e.g. breaking into a system by taking advantage of security holes, or defacing someone else's web page)
10. Using an account that the user is not authorised to use, or obtaining a password for a computer account without the consent of the account owner.
11. Providing any assistance to any person to facilitate unauthorised access to one or more files, accounts, computers, network devices or network segments.
12. Deliberate wasting of computer resources, but not limited to, like Internet bandwidth, CPU time, or excessively large (much more than 20-30 pages) print-outs. Please note that download of movies, music, on-line watching of movies or listening to music are disallowed. Download / upload using peer to peer protocol, visiting porno sites etc. is forbidden as is printing of text books, story books etc. Running of

jobs not connected with Fakir Mohan University work/projects on computation severs is a similar deliberate misuse.
13. Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing or deleting another user's files or software without explicit agreement of the owner.
14. Preventing others from accessing services.
15. Sending forged messages under someone else's name.
16. Employing a false identity for e-mail or other purposes.
17. Using email to harass others.
18. Charging the services availed of by a person to the account of another.

5.2 Degree of Punishment

The degree of punishment for the said misuses is suspension of computer and access of ICT facilities for six months and cases being sent to concerned authorities for disciplinary action along with imposition of financial fine.

6. **Policy Implementation and Monitoring**

A committee Chaired by Hon'ble Vice Chancellor of Fakir Mohan University will be formed to monitor the policy implementation. This committee would meet once in a year to take stock of the implementation of the policy with respect to its targets and objectives.

An operational guideline for grounding this policy would be prepared by Office-in-Charge along with other members of Central Computing Facilities center at the quickest as possible.

7. **Miscellaneous**

This policy will be in force until 31st March 2025 or till substituted by another policy on the recommendation of the apex body (Syndicate) of the University. The University may at any time amend any provision of this policy with due approval of apex body (Syndicate) of the University.

8**. Definitions and Abbreviations**

University means Fakir Mohan University, Balasore, Odisha.
IT/ICT includes computer science

IT: Information Technology
ICT: Information and Communication Technology
CS: Computer Science.
CCFC: Central Computing Facility Center
FMU: Fakir Mohan University
AMC: Annual Maintenance Contract