INFORMATION TECHNOLOGY POLICY

TABLE OF CONTENTS

1. SCOPE OF THE POLICY

The Information Technology Policy (IT Policy) of Manonmaniam Sundaranar University attempts to govern the users of the Information Technology Enabled Systems (ITES) created by the University for the purpose of educational supplementary services to the students and teachers; administrative support services to the administrative staff; and information and interactive services to all stakeholders of the university.

2. OBJECTIVES OF THE POLICY

The main objective of the policy is to ensure appropriate and effective usage of the ITES of the University by the stake holders.

Further the policy covers the ways and means -

- ❖ To upgrade the ITES at par with the technologically advanced institutions
- ❖ To encourage the utilisation of the ITES
- ❖ To provide all information required by the stakeholders through repository
- ❖ To improve public perception through social media
- ❖ To prevent the misuse by the users
- ❖ To take necessary corrective measures against breach

3. COMPUTING CENTRE

a. Website Management

This section of the policy deals with all the relevant technical issues related to the institution's website.

i. Website Registration

The office of the MSU-Center for Computingshall maintain a website register that has the recordsof the following details:

- List of domain names registered to the institution,
- Dates of renewal for domain names,
- Details of hosting service providers and the relevant payments, and
- Expiry dates of hosting

Keeping the register up to date, renewals,and payments against the items listed in the record are the responsibility of the Director, Center for Computing.

ii. Content Management

All content on the institution's website must be checked for their accuracy, relevance, and updation. The Director, Center for Computing, or any authorized individual designated by MSU authorities will be solely responsible for maintaining the contents in the website. Heads of departments /sections who provide the information will be responsible for the contents in the website. The website's content should be evaluated/reviewed on daily / time to time depends on their nature.

The Director, Center for Computing or any MSU technical personnel acting on the Director's direction can modify the institution's website's content and their links. Faculty members / sections shall send updates to the Centre for computing to upload & update the website. Care is to be taken to ensure information available on the website is accurate as it is always considered to be authentic. Heads of the Departments and Heads of the division /section are responsible for the authenticity of the information which is available on the website pertaining to their department or division/ section.

To establish a consistent and unified image for the institution, web pages shall adhere to basic branding guidelines. The Privacy and Copyright Act applies to all content on the website.

iii. Website Disruption

If the institution's website is disrupted, the following actions shall be taken promptly:

- Notify the Registrar and Vice Chancellor immediately;
- Notify the website host; and
- The technical team / service provider of MSU shall respond swiftly to the emergency and carry out the directives of university officials.

b. Internet Connectivity

The MSU Campus Internet Connectivity will be designed, implemented, and maintained by the Center for Computing.

The Center for Computing will allocate a static IP address to all devices on the MSU network and reserve the right to change these assigned addresses at any time with due notice to the user.

An official request for an IP address shall be made to the Center for Computing, and once granted, the address must be posted on the CPU through a sticker.

The individual user should not change an address allocated to a device, nor should the same address be used on any other widget, even if the other device belongs to the same user or department.

IP addresses can also be obtained dynamically from the centrally managed DHCP server. The Center for Computing will decide to allot static or dynamic IP addresses based on need.

No services such as HTTP, HTTPS, FTP, or DHCP shall be run at the department level without the prior consent of the Center for Computing.

Wireless LAN will be provided wherever possible. A centrally run DHCP server will provide the IP for the wireless LAN.

No devices, such as routers, switches, access points, or software hotspots, which have a bearing on network security are allowed to be connected to the MSU network without prior consent from the Center for Computing.

Efforts will be made to provide WLAN everywhere on campus, but there may be variations in signal strength, and WLAN coverage shall not be claimed as a matter of right by any user.

WLAN will normally be provided for registered MSU users. However, WLAN may also be extended to guests visiting MSU with authorization from the respective authority.

The Center for Computing will generate guest access keys on prior request and hand them over to the respective departments. Departments are responsible for maintaining the users' credentials on a logbook before allotting the keys.

WLAN may also be temporarily provided at locations where wireless access points exist for group access to participants attending official conferences and seminars, etc., on a formal request to the center for computing at least 3 working days in advance of the event by the respective authority. Users will be granted WLAN access after registering their device with the Center for Computing.

Departments shall send a list of students enrolled in their respective departments at the beginning of the academic year to the Center for Computing.

Wireless devices that do not have antivirus software will be denied WLAN access.If any virus activity is noticed on an active wireless device, the device will be disconnected from the WLAN, even if it is virus-free. The individual owner of the device will be solely responsible for cleaning the machine from viruses.

The Center for Computing will register the device on WLAN and is not responsible for rectifying networking or software faults arising within the device during the time of registration.

The device information will be noted, and the user will be continuously provided WLAN access for not more than two years for students. After the period expires, the device needs to be re-registered, if needed. The individual user should approach the Center for Computing again for re-registration.

Hostels will be provided with WLAN facilities only at a common location identified by the hostel committee.

Students will be allowed WLAN on laptops, desktops (in the case of hostel residents), and notebooks only. No students will be provided with WLAN on their mobile devices.

Faculty members and officers of the University may normally be provided with connections on approved university devices (desktops and laptops) by the respective

authority. In addition, they may normally be permitted to register only one personal mobile device. Requests for additional connections may be made formally to the Center for Computing for consideration.

c. E-Mail Management

Email services are not a right but rather a privilege. The official email address provided to academics, employees, and students may only be used for administrative and academic purposes. Every email user of our University's domain is required to abide by and adhere to the email policy. Access restrictions at the IP address, domain, email, group level, associated app, etc., or any other conditions deemed appropriate by the administration may be imposed from time to time on any university employee, student, or group in the larger interest, and these restrictions will be binding on all users. The campus community's attention is brought to the Information Technology Act of 2000 and the Information Technology (Amendment) Act of 2008. Obviously, all community members will be bound by the aforementioned.

Electronic mail is a university-provided service that serves as a key means of communication while improving education and administrative efficiency. Users are responsible for using this resource efficiently, ethically, and legally. The official communication shall be send from various offices of the university through this mail IDs. Using official email accounts demonstrates the user's acceptance of this policy.

i. Account Creation

University E-mail Accounts are created based on the official name of the staff / section. Student accounts shall be created to their registration number. Faculty, staff, or departments may seek temporary email privileges for special events. Faculty or Staff requesting these types of accounts shall submit user information, reason for the account, expiration date, and sponsor-information along with their request to the Registrar.

ii. Ownership of Email Data

The University owns all University Email Accounts. Subject to underlying copyright and other intellectual property rights under applicable laws and University policies, the University also owns data transmitted or stored using the University Email Accounts.

iii. Privacy and Right of Institute Access

While the University will make every attempt to keep email messages secure, privacy is not guaranteed. Users should have no general expectation of privacy in emails sent through university email accounts. Under certain circumstances, it may be necessary for the Director, Center for Computing (with sufficient orders from the Registrar, MSU) to access institute email accounts. These circumstances may include, but are not limited to, maintaining the system, investigating security or incidents of abuse, investigating violations of this or other University policies, or, in the case of Gmail accounts, breaches of Google's Acceptable Use Policy or the University's contracts with Google. The Director Center for Computing (with sufficient orders from the Registrar MSU) may also require access to the University Email Account in order to continue University business where the University Email Account holder will not or can no longer access the University Email Account for any reason (such as death, disability, illness, or separation from the University for a period of time or permanently). Such access will be on an as-needed basis. Any email accessed will only be disclosed to individuals who have been appropriately authorized and have an appropriate need to know or as required by law. MSU and Google's applicable acceptable use policies bind all email users. Google also retains the right to access Gmail accounts for violations of its fair use policy.

iv. Data Purging

Gmail, G-suite Accounts (with University domain) Email messages held under Gmail Accounts will be subject to Google's storage and retention policies, which may change from time to time, with or without notice. Individuals should not rely on an email account to archive data; each person is responsible for saving individual messages and attachments as appropriate.

v. Data Backup

University Email Accounts are not backed-up. The Center for Computing room or University is not responsible for any data loss.

vi. Expiration of Accounts

Individuals may leave the University for various reasons which gives rise to different situations regarding the length of email privileges or expiration of accounts. The policy governing those privileges is set forth below. Notwithstanding the guidelines below, the University reserves the right to revoke email privileges at any time. Invariably, an email account is deactivated/suspended within one week of the member leaving the University (with due notification to the user).

vii. Inappropriate Use

The exchange of any illegal email content specified below and described elsewhere in this policy is forbidden with respect to University Email Accounts. Users who receive such emails should report to Center for Computing immediately or send an email to ic@msuniv.ac.in. Serious complaints will be investigated, and if appropriate, such infractions will be handed over for further investigation and action will be taken in accordance with the law of the land.

The exchange of any email content as outlined below is prohibited:

- Generates or facilitates unsolicited bulk email;
- Infringes on another person's copyright, trade or service mark, patent, or other property right or is intended to assist others in defeating those protections;
- Violates or encourages the violation of, the legal rights of others or federal and state laws;
- Is for any malicious, unlawful, invasive, infringing, defamatory, impersonating, or fraudulent purpose;
- Intentionally distributes viruses, worms, Trojan horses, malware, corrupted files, hoaxes, or other items of a destructive or deceptive nature;
- Alters, disables, interferes with, or circumvents any aspect of the email services;
- Tests or reverse-engineers the email services to find limitations, vulnerabilities or evade filtering capabilities;
- Constitutes, foster, or promotes pornography;

- Creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security, or interferes with an investigation by law enforcement;
- Improperly exposes trade secrets or other confidential or proprietary information of another person;
- Misrepresents the identity of the sender of an email;
- Using or attempting to use the accounts of others without their permission;
- Collecting or using email addresses, screen names information, or other identifiers without the consent of the person identified (including, without limitation, phishing, spidering, and harvesting);
- Use of the service to distribute software that covertly gathers or transmits information about an individual;
- Conducting business for profit under the aegis of the University; and
- Political activities include supporting a candidate's nomination for political office or attempting to influence the vote in any election or referendum on behalf of or with the University's sponsorship.

This list is not intended to be exhaustive but to provide some illustrative examples.

d. Firewall and Anti Virus

Internet traffic will be monitored and filtered centrally.Site filtering shall be done based on website category. The UTM (Unified Threat Management) and firewall vendor will decide a website category based on the advisory committee's recommendation. The categories of sites like Pornography, Malicious sites, Proxy avoidance, Spam URLs, Hate and crimes, Dating, Gambling,Games, Unrated, and Any other site deemed undesirable by the MSU administration from time to time will be permanently blocked.

Students' requests for whitelisting a particular site shall be forwarded through the head of the department. Teachers and officers may send their requests for site listing directly to the Registrar. The IT Committee / Center for Computing committee shall examine the request and take actions appropriately.

Incorrectly rated or unrated sites shall be brought to the Center for Computing's attention via a note or email.The issue will be resolved as soon as possible.

Some sites, such as online shopping, entertainment, news, and media, will be disabled for all users during university working hours. During office hours, access to the Internet will be restricted to educational sites, government sites, and email. All other permissible websites will be open only during non-working hours. However, a head wanting to provide access to any computers or staff may do so through a special written request to the Center for Computing.

Interferes with the use of the email services or the equipment used to provide the email services by an individual and / or any deliberate attempt by an individual to bypass the firewall or web filter through any process or software or to breach firewall or wireless security by any means will be liable for disciplinary action, including debarring from further use of the MSU Network and a monetary fine double the amount of perceived damage determined by the committee.

Antivirus shall be purchased by center for computing for bulk usage and be installed in all systems used in the departments and sections. The renewal of the same shall be done periodically.

e. Maintenance of Log

A logbook of all the IP addresses allocated is to be maintained by the respective departments or section.All the traffic on the network shall be logged and monitored centrally on the firewall, switches, and servers.All logs will be kept on the device as per the availability of space on servers or 30 days whichever occurs earlier. The log details that are related to discrepancies in the usage need to be kept until the issue is resolved. The information regarding the log shall be presented only to Committees and Authorities on written direction by the Registrar.

f. Intercom Management

The Center for Computing will construct and maintain the MSU Campus PBAX system.On request, the Center for Computing will assign Connections to persons and offices

via proper channels.The center for computing will do any necessary maintenance, expansion, or updating.

g. Surveillance

Notify staff, students, and parents of this surveillance policy in writing. Consider making security cameras visible. The security cameras shall be maintained at common places namely main entrances and exits, public access areas, storage areas, parking lots, examination and research wings and cafeterias.

The following are the goals of surveillance.

- To detect trespassers, unauthorized individuals, and unauthorized vehicles on university premises and suspicious activity on campus after hours.
- Aid the on-campus securities' ability to monitor and respond to incidents on campus quickly.
- In the event of a conflict, hold the correct parties responsible and find evidence of what took place and take appropriate action.

Besides practicing strong cyber security protocols, the authorized person nominated by the university authorities only have access to the footages. The footages shall be retained for one month. In case conflicting incidents, the footages shall be copied in a separate storage device and be handed over to the Registrar for further reference.

4. LEARNING MANAGEMENT SYSTEM

Manonmaniam Sundaranar University has its own Institutional Learning Management System namely "MSULMS". The website address is http://msunivlms.in.

This policy applies to all the users of MSULMS at Manonmaniam Sundaranar University. The responsible unit for the MSULMS is Centre for Online Education with specific management oversight.

The administrators, syndicate members, faculty members, research scholars, students and administrative staff are allowed to use the MSULMS. In order to access the MSULMS,

every user will be given the login credentials (Login ID and Password). The user can able to access the site by using the login credentials assigned to them. Based on the role, the privileges are assigned.

a. Infrastructure requirement

Policies for effective use of MSULMS

- The server shall be kept in a safe and secured room with 24 X 7 power backup and air-condition facility.
- At regular intervals, data back-up shall be madein a mirror server that is to be maintained for the data backup.
- The cable connections shall be properly maintained and regular maintenance of supportive electrical components such as UPS, Battery shall be installed.
- Fire safety equipments must be available in Server room, in condition.
- Updation shall be made as and when required

b. Content Management

Content means the e-content developed by the teacher for the specific course/ programme like workshop or training.

A teacher can have 1 to 5 courses per semester. The course site size limit is one 1 gigabyte. This does not include student assignments and discussion. If needed, additional space may be allotted to the course based on the written request.The faculty members are responsible for the e-contents developed by them. The unplagiarized contents shall be posted in the LMS. The unused e-contents shall be deleted by the teacher concerned. If any content is found as unused for more than a year, it will be deleted by the administrator with prior notice to the teacher.

Every course page shall be maintained for oneacademic year. After the retention period has expired, the course page will be deleted. If needed, a request shall be submitted by the teacher to retain the course for specific period of time.

The Administrator shall be allowed to enter into any course page for troubleshooting purposes.

c. User management

The role-based policies are as follows:

Administrator: A role is assigned to the person(s) who oversee and manage the user accounts and admin accounts. The Admin shall create course page, add, view and moderate enrollments and content for all courses, view course and log data, and manage course-level user roles and permissions. The LMS Admin role is managed by Centre for Online Education.

Teacher: The faculty member has to send the request to create a course page along with the details such as course name and participants' details including name of the participant and email id. The request and details shall be sent to msudigitallearning@gmail.com . The details shall be validated and the course page shall be created. The creation of course page shall be communicated to the faculty member concerned through email. The content shall be posted in MSULMS by the faculty member directly.

Guest : An account created by the LMS Administrator in order to grant an external user affiliated with the university access to the MSULMS.

5. MANAGEMENT INFORMATION SYSTEM

Management Information Centre of Manonmaniam Sundaranar University automates the office process and create a digital repository for storing the information about the employees.In MIS, role based login credentials are created and based on the role, the privileges are assigned.All employees of MS University must enter their details such as personal details, educational qualification, designation details, etc. in this MIS using the linkwww.msuniv.ac.in(or)http://14.139.186.246:8080/MIS/

The higher officials such as Vice-chancellor and Registrar can able to view the data entered by the various sections and faculty members of various departments. The faculty members shall enter the academic related data such as Ph.D. guidance, Patents filed, Book written, Papers published, Countries visited, Conferences attended/ organized, Seminar attended/organized and etc. in MIS. The administrative staff shall enter the work related data such as the positions, sections, duration in each section, responsibility, tapals dealt, etc.

For tapal tracking purpose, the tapals received by the University shall be entered by the responsible staff in MIS. The further actions on Tapal shall be updated in every stage of the tapal movement till disposal.

Internal Quality Assurance Cell (IQAC) shall conduct the training programme for the faculty members and administrative staff to learn MIS utilisation.Management Inforamtion Centre and Centre for Online education shall also conduct training programmes on MIS and LMS to enter the data in MIS and handle LMS properly.

6. PUBLICITY THROUGH SOCIAL MEDIA

The primary goal of this policy is to protect the University from any unanticipated adverse consequences of social media use by University personnel and students. It also strives to inform social media platform users about their roles, responsibilities, and obligations under the University's Social Media Policy.

This policy applies to all staff of the University (including temporary workers and other appointees) and to all communications on social media which directly or indirectly represent or impact the University, its staff, and students.

Social media networks accounts of the University and its constituent sections aims to communicate with diverse audiences and stakeholders. These channels allow staff and students to utilize various professional and personal possibilities. The users shall take care that the University's reputation in the long run is enhanced considerably.

All Official University Social Media Sites must respect intellectual property rights, the Copyright law of India,and the University rules and regulations. If the user is not representing the University but using social media for personal reasons and identify themselves as a University employee, the user has to give a disclaimer such as, "Views and opinions expressed are my own and do not reflect that of my employer."

Use of social media must not infringe on the rights, or privacy, of the students or staff, and staff/students must not make ill-considered comments or judgments about other students, staff or third parties. The University will not accept any form of bullying or harassment by or of members of the University, students, or stakeholders using new media tools.

Any individual suspected of violating this policy will be required to cooperate with any investigation in accordance with the disciplinary procedure. Non-cooperation may lead to further disciplinary action.

Individual have to remove internet or social media posts on request by the University that the University finds to be in breach of the policy. Failure to comply with such a request may result in further disciplinary action.

The University is not responsible for and does not own any content posted on social media by its stakeholders, on their own.

Every student at the time of admission must sign an undertaking on social media usage along with anti-ragging and other formalities.

7. PURCHASE, RENEWAL AND DISPOSAL OF HARDWARE AND SOFTWARE

Purchase of any hardware and / or software need to be done by following the purchase norms of the University and Government of Tamilnadu which are formulated / revised, time to time. The availability of hardware and software details shall be maintained in a centralised database to enable sharing of resources in effective manner and to avoid duplication of purchase of resources. The renewal and up-gradation of software licenses shall be done periodically and copies of the licenses to be kept for verification at any point of time. Users shall be motivated to use a licensed software or freeware and to avoid pirated software.

The disposal of the electronic waste is to be done by following the norms as stated in the Government Order Number 9 dated 23.04.2013 or later versions, as applicable.

8. E-REPOSITORY

MSU intends to post as much academic and administrative material as possible on its official website. As part of its open access for public information, these will contain e-repositories of faculty members' publications/presentations, dissertations, and theses.E-repositories shall be created and maintained by the Library, IQAC, and / or Center for Computing. The Center for Computing will host these repositories on MSU-MIS servers.

Content: If the author's affiliation in the publication indicates MSU, all works by faculty members and students will be placed in the MSU repository. Any retired faculty member who still uses the MSU affiliation in their publications would also be included in the e-repository. On the other hand, a paper/document published by a faculty or student with another affiliation will not be included in MSU's e-repository.

9. DEMANDS & COMPLAINTS

Any system used by many stakeholders requires modifications to cater the new requirements and to curtail wrong usage of the facilities. Everyone who utilise the Information Technology system of the University may give their suggestion to the authorities of the Universities on their need with justification through the proper channel (Students and Members of the faculties through the Head of the Department and Dean; and Administrative staff through the section heads and AR / DR). On scrutinising the demands, the final decision on the requirement be decided by the authorities.

Whenever, misuse of the system is identified by any stakeholder, they may bring the issue as complaint against the provision available in the system. Such complaints received are to be dealt within a week by the authorities.

A prescribed form for the demands / complaints through proper channel be submitted to the Registrar. A Monitoring Committee comprising the following combination be formulated to consider and recommend action with respect to the demands and complaints.

i. Member Syndicate

ii. All Deans of Faculties / Chairpersons of Schools

iii. One Professor

iv. One DR / AR

v. Two Administrative staff at the level of Junior Assistant / Assistant

vi. Two Student representatives

The committee shall meet whenever any demand / complaint is received or once in six months, whichever is earlier. The committee may, of its own, give suggestions to upgrade the Information Technology System in the University and also add, amend and/or delete any of the clauses given in the policies.

10. BREACH OF THE POLICY

Any inappropriate use of the Information Technology system of the University is considered as breach. The inappropriate use of the system is to be identified from the log created in the computing centre. On identifying any inappropriate use, the system administrator has to report the issue regarding the user and usage pattern to the Registrar which in turn will be directed to the Monitoring Committee dealing with demands and complaints.

Inappropriate use of the system includes – attempting to visit websites which are barred by the firewall; logging in to the system with more than the permitted number of systems; misusing others' login credentials; altering IP details; sharing confidential data; and such others.

11. REVISION OF THE POLICY

Any doubt or dispute about the interpretation of these policies shall be referred to the Vice Chancellor, whose decision in his capacity as the chair person of Syndicate shall be final.The Vice Chancellor is authorized to add, amend and/or delete any of the clauses given in the policies and to formulate a committee to revise the policy which shall be further reported to Syndicate at its next meeting for ratification.

REGISTRAR
MANONMANIAM SUNDARANAR UNIVERSITY
TIRUNELVELI - 627 012.