UNIVERSITY OF SCIENCE & TECHNOLOGY MEGHALAYA

Unveiling Excellence

USTM

IT Policy & Charter

(Chapter - XIX, University Policies & Guidelines)

Fast
Transparent
Networking
Accessible
Sharing

CHAPTER XIX

IT POLICY & CHARTER

Table of Contents

Introduction:

The USTM IT Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the institution which must be followed by all staff. It also provides guidelines USTM will use to administer these policies, with the correct procedure to follow.USTM will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures.Any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome.

These policies and procedures apply to all employees.

1. Need for IT Policy

- Basically the University IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the University on the campus.
- This policy establishes University-wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the University.
- Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information.

2. Responsibilities of Information Technology & Network Unit (ITNU)

The campus network backbone and its active components are administered, maintained and controlled by ***Information Technology & Network Unit (ITNU)***

ITN Unit operates the campus network backbone such that service levels are maintained as required by the University Sections, departments, and divisions served by the campus network backbone within the constraints of operational best practices.

3. IT Hardware Purchasing & Installation Policy

- Computer hardware refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and RAM. External hardware devices include monitors, keyboards, mice, printers, and scanners.
- University network user community needs to observe certain precautions while getting their computers or peripherals installed so that he/she may face minimum inconvenience due to interruption of services due to hardware failures.

4. Open Source Policy

Open source software (OSS) in one of the least expensive and most effective solutions for technology and knowledge transfer since its helps to monitor and regulate access to resources and to create web-accessible data bases and applications.

Objective:

- To provide a policy framework for rapid and effective adoption OSS
- To ensure strategic control in applications and systems from a long term perspective.
- To encourage contribution to the development of OSS among the academia.

Policy Statement:

USTM shall Endeavour to adopt open source software (OSS) in all teaching, research and administrative activities as a preferred option in comparison to closed source software.

5. Software Purchasing, Installation & Licensing Policy

Purchase of software:

- The purchase of all software must adhere to this policy.
- All purchased software must be purchased by establishment officer with recommended from IT officer
- All purchased software must be purchased from reputed software seller.
- All purchases of software must be supported by proper license and be compatible with the institution's server and/or hardware system.
- Any changes from the above requirements must be authorised by registrar
- All purchases for software must be in line with the purchasing policy in the financial policies and procedures manual.

Installation & Licensing:

- Any computer purchases made by the individual departments/administrator should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software)installed.
- Respecting the anti-piracy laws of the country, University IT policy does not allow any pirated/unauthorized software installation on the university owned computers and the computers connected to the university campus network.
- Where licensing states limited usage (i.e. number of computers or users etc.), then it is the responsibility of IT officer to ensure these terms are followed.IT officer is responsible for completing a software audit of all hardware twice a year to ensure that software copyrights and license agreements are adhered to.
- All computer software copyrights and terms of all software licences will be followed by all employees of the institution. In case of any such instances, university will hold the department/individual personally responsible for any pirated software installed on the computers located in their department/individuals' rooms.

6. Network (Intranet & Internet) Use Policy

- Network connectivity provided through the University, referred to hereafter as "the USTM Network", either through an authenticated network access connection or a Local Area Network (LAN) connection, is governed under the University IT Policy.
- The ***Information Technology & Network Unit (ITNU)*** is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the University's network should be reported to the team.

7. Email Account Use Policy

- In an effort to increase the efficient distribution of critical information to all faculty, staff and students, and the University's administrators, it is recommended to utilize the university's e-mail services, for formal University communication and for academic & other official purposes.
- E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals.

8. Bring Your Own Device Policy

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

❖ Purpose of the Policy:

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

❖ Procedures:

- Employees when using personal devices for institution use will register the device with ITNU
- ITNU will record the device and all applications used by the device.
- Personal mobile devices can only be used for the following institution purposes:
- Insert each type of approved use such as email access, institution internet access, institution telephone calls etc.

❖ Each employee who utilises personal mobile devices agrees:

- Not to download or transfer institution or personal sensitive information to the device.
- Not to use the registered mobile device as the sole repository for USTM's information. All institution information stored on mobile devices should be backed up
- To make every reasonable effort to ensure that USTM's information is not compromised through the use of mobile equipment in a public place and all registered devices should be password protected
- Not to share the device with other individuals to protect the institution data access through the device
- To abide by USTM's internet policy for appropriate use and access of internet sites etc.
- To notify USTM immediately in the event of loss or theft of the registered device

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

- Owns all intellectual property created on the device
- Can access all data held on the device, including personal data
- Will delete all data held on the device in the event of loss or theft of the device
- Has the right to deregister the device for institution use at any time.

9. Web Site Hosting Policy

Publicly accessible web pages presenting university information must be hosted within the universities content management system. This policy, approved by the University of Science & Technology, Meghalaya, establishes a central web hosting policy for all faculty and staff within the college.

As on date, the university's webmaster is responsible for maintaining the official web site of the university viz., http://www.ustm.ac.in only.

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

❖ Procedures:

❖ Website Register

The website register must record the following details:

- List of domain names registered to the institution
- Dates of renewal for domain names
- List of hosting service providers
- Expiry dates of hosting

❖ Website Content

- All content on the institution website is to be accurate, appropriate and current. This will be the responsibility of ITNU
- All content on the website must follow University rules
- The content of the website is to be reviewed routinely.
- Basic branding guidelines must be followed on websites to ensure a consistent and cohesive image for the institution.
- All data collected from the website is to adhere to the Privacy Act

10. University Database Use Policy

Data is a vital and important University resource for providing useful information. Its use must be protected even when the data may not beconfidential. USTM has its own policies regarding the creation of database and access to information and a more generic policy on data access. Combined, these policies outline the university's approach to both the access and use of this universityresource.

11. Electronic Transactions Policy

❖ Purpose of the Policy:

This policy provides guidelines for all electronic transactions undertaken on behalf of the institution.

The objective of this policy is to ensure that use of electronic funds transfers and receipts are started, carried out, and approved in a secure manner.

❖ Procedures:

✓ Electronic Funds Transfer (EFT)

- It is the policy of USTM that all payments and receipts should be made by EFT where appropriate.
- All EFT payments and receipts must adhere to all finance policies in the financial policies and procedures manual.
- All EFT arrangements, including receipts and payments must be submitted to {insert relevant department of the institution here, e.g. finance department}.
- It is the responsibility of finance officer to annually review EFT authorisations for initial entry, alterations, or deletion of EFT records, including supplier payment records and customer receipt records.

❖ Electronic Purchases

- All electronic purchases by any authorised employee must adhere to the purchasing policy in the Financial policies and procedures manual.
- Where an electronic purchase is being considered, the person authorising this transaction must ensure that the internet sales site is secure and safe and be able to demonstrate that this has been reviewed.
- All electronic purchases must be undertaken using institution credit cards only and therefore adhere to the institution credit card policy in the Financial policies and procedures manual.

12. IT Service Agreements Policy

❖ Purpose of the Policy:

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

❖ **Procedures:**

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

- Provision of general IT services
- Provision of network hardware and software
- Repairs and maintenance of IT equipment
- Provision of institution software
- Provision of mobile phones and relevant plans
- Website design, maintenance etc.

✓ All IT service agreements must be reviewed by legal officer/expert before the agreement is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by registrar

✓ All IT service agreements, obligations and renewals must be recorded in IT record registrar

✓ Where an IT service agreement renewal is required, in the event that the agreement is substantially unchanged from the previous agreement, then this agreement renewal can be authorised by registrar

✓ Where an IT service agreement renewal is required, in the event that the agreement has substantially changed from the previous agreement, legal officer before the renewal is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by registrar

✓ In the event that there is a dispute to the provision of IT services covered by an IT service agreement, it must be referred to legal officer who will be responsible for the settlement of such dispute.

13. Emergency Management of Information Technology

❖ **Purpose of the Policy**

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

❖ **Procedures:**

➢ IT Hardware Failure

- Where there is failure of any of the institution's hardware, this must be referred to ITNU immediately.
- It is the responsibility of ITNU to access/manage/repair in the event of IT hardware failure.
- It is the responsibility of IT officer to undertake tests on planned emergency procedures recommended quarterly to ensure that all planned emergency procedures are appropriate and minimise disruption to institution operations.

➢ **Virus or other security breach**

- In the event that the institution's information technology is compromised by software virus or any web attack such breaches are to be reported to ITNU immediately.
- ITNU is responsible for ensuring that any security breach is dealt with within 48 hours to minimise disruption to institution operations.

➢ **Website Disruption**

- In the event that institution website is disrupted, the following actions must be immediately undertaken:
- Website host to be notified
- IT officer/registrar must be notified immediately

It should be noted that even with all the procedures listed above, there is still some possibility of any kind of issue/complication and which will be periodically reviewed by the higher authority.

Drafted by a committee consisting of

1. Dr Bairab Sharma HOD (Computer Science)
2. Mr Jainul Abudin, Associate Prof (Computer Science)
3. Mr R Prodhani, Asst Prof (Computer Science)
4. Mr Shamim Goney, Deputy Registrar (Admin)

Campus
Techno City, Khanapara, Kling Road, Baridua, 9th Mile, Ri-Bhoi, Meghalaya-793101
Ph. 0361-2895030,E-mail : ustm2011@gmail.com
Web : www.ustm.ac.in

Amenity Centre