SIKKIM MANIPAL UNIVERSITY

STANDARD OPERATING PROCEDURE AND KEY POLICIES FOR SMU-IT

POLICY DOCUMENT

To ensure an information technology infrastructure that promotes the basic missions of the University in teaching, learning, research, patient care, and administration

Author			
Name	Role	Date of Preparation	Signature
Siddesh B. Desai	Management Trainee	22/06/2009	
Contributor(s)			
Name	Role		Signature
Mr. Zareef ahmad	System Analyst		
Mr. Nihar Ranjan Sahu	System Analyst		
Mr. Ranjit Panigrahi	System Analyst		
Mr Om Shankar Dwivedi	Jr. System Analyst		
Mr. Avijit Karmakar	System Administrator		
Reviewer			
Name	Role	Date of Approval	Signature
Mr. Nihar Ranjan Sahu	System Analyst	13/08/2009	
Document Path	Version Number	Date of Release	
	1.0	13/08/2009	

Revision History			
Version Number changed From To	Date of Release	Section/ Page # Changed	Details of Changes
0 -- 1.0	13/08/2009	First Release	First Release

Purpose:

The purpose of this Policy is:

1. To ensure an information technology infrastructure that promotes the basic missions of the University in teaching, learning, research, patient care, and administration. In particular, this Policy aims to promote the following goals:
    a. To ensure the integrity, reliability, availability, and superior performance of IT Systems;
    b. To ensure that use of IT Systems is consistent with the principles and values that govern use of other University facilities and services;
    c. To ensure that IT Systems are used for their intended purposes; and
    d. To establish processes for addressing policy violations and sanctions for violators.

2. To ensure professional, ethical and lawful business use of IT infrastructure such as computers, e-mail, and computer networks (both internal and external), including fax machines, telephones and to prevent potential abuse. **It is important that each user of the Company's computer and communications systems read and understand the provisions of this policy in order to minimise the risk, to both the employee and the Company, arising from the abuse or misuse of these systems**. All users of these systems will be considered to have read this policy and will be expected to comply with its provisions.

Definitions:

IT Systems: These are the computers, internet, terminals, printers, networks, modem banks, online and offline storage media and related equipment, software, and data files that are owned, managed, or maintained by University. For example, IT Systems include institutional and departmental information systems, faculty research systems, desktop computers, the University's campus network, and University general access computer clusters.

User: A "User" is any person, whether authorized or not, who makes any use of any IT System from any location. For example, Users include a person who accesses IT Systems in a University computer cluster, or via an electronic network

Systems Administrator: Systems Authorities may designate another person as "Systems Administrator" to manage the particular system assigned to him or her. Systems Administrators oversee the day-to-day operation of the system and are authorized to determine who is permitted access to particular IT resources.

Coverage:

These policies cover the usage of all of the Company's Information Technology and communication resources, including, but not limited to:

• All computer-related equipment, including desktop personal computers (PCs), portable PCs, terminals, workstations, wireless computing devices, telecomm equipment, networks, databases, printers, servers and shared computers, and all networks and hardware to which this equipment is connected

• All electronic communications equipment, including telephones, communicators, fax machines, wired or wireless communications devices and services, Internet and intranet and other on-line services

• All software including purchased or licensed business software applications, Company-written applications, employee or vendor/supplier-written applications, computer operating systems and any other software residing on Company-owned equipment

• All intellectual property and other data stored on Company equipment

• All of the above are included whether they are owned or leased by the company or are under the company's possession, custody, or control

• These policies also apply to all users, whether on Company property, connected from remote via any networked connection, or using Company equipment

Covers all employees including temporary staff who use computers / laptops for discharging their work / duties. It is the responsibility of all operating units to ensure that these policies are clearly communicated, understood and followed.

Rights granted:

a) Administrator on behalf of the Company will allocate facilities based on entitlements that are roles and authorizations.

b) Administrator on behalf of the Company reserves the right to grant, or with or without cause or notice to employee withdraw, suspend or alter such allocations at its sole discretion.

c) Every allocation of facility will be entertained only after proper authorization is obtained

Preferred modes and passwords:

a) Email facilities should be the preferred medium of communication within the Company.

b) More expensive methods of communication like telephones, facsimile and paper based communication must be avoided as far as possible.

c) **Personal Account Responsibility**. Users are responsible for maintaining the security of their own IT Systems accounts and passwords. Any User changes of password must follow published guidelines for passwords. Accounts and passwords are normally assigned to single Users and are not to be shared with any other person. Users are presumed to be responsible for any activity carried out under their IT Systems accounts or posted on their personal web pages and users will be finally accountable for any mail/information/action that can be traced to his/her account

1.4 Drafting precautions:

a) Employees should exercise care in drafting e-mail, communicating in chat groups, and posting items to newsgroups as they would for any other written communication.
b) Anything created on the computer or Internet may, and often will, be reviewed by others.
c) Please scan for viruses and other destructive programs before placing them onto the Company's computer systems. Also scan for viruses on the material downloaded from the Internet or from computers or networks that do not belong to the Company.

d) Without specific authorization, Users must not physically or electrically attach any additional device (such as an external disk, printer, or video system) to IT Systems. By attaching privately owned personal computers or other IT resources to the University's network, Users consent to Information Systems department use of scanning programs for security purposes on those resources while attached to the network.

e) Installation of any software including purchased or licensed business software applications, Company-written applications, employee or vendor/supplier-written applications, computer operating systems, and any other software residing on Company-owned equipment without proper authorization from the administrator is not permitted

f) Modification or removal of data or equipment. Without specific authorization, Users may not remove or modify any University-owned or administered equipment or data from IT Systems.

g) Unauthorized access or use. The University recognizes the importance of preserving the privacy of Users and data stored in IT systems. Users must honor this principle by neither seeking to obtain unauthorized access to IT Systems, nor permitting or assisting any others in doing the same. Users are prohibited from accessing or attempting to access data on IT Systems that they are not

authorized to access. Furthermore, Users must not make or attempt to make any deliberate, unauthorized changes to data on an IT System.

h) Responsibility for Content. Official University information may be published in a variety of electronic forms. The Certifying Authority under whose auspices the information is published is responsible for the content of the published document.

Business Use:

1.5 a) The Company's computer and communications systems are exclusively for business purpose.
1.5 b) Employees should not consider messages and data sent from, received by, or stored in or upon Company computer and communications systems to be private and should not send, receive, or store sensitive personal or private information using these systems as all these messages and data are the sole property of the Company, regardless of the form and/or content.

1.6 Company proprietary rights:

The company shall exclusively own all rights in and to materials, including patentable inventions, copyrights, and trade secrets, developed using the Company's computer and communications systems.

a) Conditions of University access

University may access all aspects of IT Systems, without the consent of the User, in the following circumstances:

1. When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the IT Systems; or

2. When required by central, state, or local law or administrative rules; or

3. When there are reasonable grounds to believe that a violation of law or a significant breach of University policy may have taken place and access and inspection or monitoring may produce evidence related to the misconduct; or

4. When such access to IT Systems is required to carry out essential business functions of the University; or

b) User access deactivations. In addition to accessing the IT Systems, the University, through the appropriate Systems Administrator, may deactivate a User's IT privileges, whether or not the User is suspected of any violation of this Policy, when necessary to preserve the integrity of facilities, user

services, or data. The Systems Administrator will attempt to notify the User of any such action.

With respect to copyright infringement, Users should be aware that copyright law governs (among other activities) the copying, display, and use of software and other works in digital form (text, sound, images, and other multimedia). The law permits use of copyrighted material without authorization from the copyright holder for some educational purposes (protecting certain classroom practices and "fair use," for example), but an educational purpose does not automatically mean that the use is permitted without authorization.

Audit and Monitoring:

1.7 a) Company may audit, monitor, and access messages and data sent from, received by, and stored upon its computers and communications systems to ensure that these systems are not abused or misused, and to ensure compliance with IT usage policy.
1.7 b) Auditing, monitoring, and access of computers and communications systems will be conducted by authorized personnel at any time, with or without notice to affected users. Information obtained during auditing and monitoring of Company computers, computer networks, and other communications systems may be disclosed to external or internally constituted legal/disciplinary/law enforcement authorities without any prior notice or consent from affected users.
1.7 c) All users will be held personally responsible for their use of the Company's computers and communications systems during both business and non-business hours. Abuse or misuse of these systems will result in disciplinary action up to and including termination of services.

Abuse and misuse examples:

The following are examples of abuse and misuse of the Company's computers and communications systems set out for your guidance:

(i) Conducting any business, personal or otherwise, which is not the business of the Company, or use of any Company computer or communications system to access information for any purpose other than the business of the Company;
(ii) Sending, posting, or otherwise disclosing confidential information, trade secrets, or other confidential and/or protected proprietary data of either the Company or its clients or customers;
(iii) Sending, posting, or otherwise disclosing information directed to or from the Company's attorneys to anyone who is not an employee of the Company;
(iv) Accessing or attempting to access another employee's computer, computer account, e-mail or voice mail messages, files, or other data

without the express consent of the employee or an authorized supervisor;

(v) Installation of any unauthorized and/or unlicensed software on Company computers, computer networks, or other communications systems;

(vi) Use of Company computers, computer networks, and/or other communications systems to make unauthorized, unlicensed, and/or illegal copies of any software;

(vii) Downloading, uploading, storing, sending, distributing, or displaying messages, files or data, the contents, titles, filenames, or headings of which are inappropriate to a business setting, including but not limited to:

(a) obscene, lewd, lascivious, or pornographic messages, graphics files, or other data;

(b) messages, graphics files, or other data intended to harass, intimidate, threaten, embarrass, humiliate, or degrade another employee or co-worker;

(c) messages, graphics files, or other data that targets an individual or groups of individuals for purposes of harassing, intimidating, threatening, embarrassing, humiliating, degrading, or discriminating against the targeted individual or group of individuals on the basis of their ethnic origin, race, gender, age, sexual preference, or disability; and

(d) Messages, graphics files, or other data that contain defamatory references or depictions of other individuals.

(viii) Unauthorized and intentional copying, destruction, deletion, distortion, removal, concealment, modification, or encryption of messages, files, or other data on any Company computer, computer network, or other communications system, including specifically the use of encryption algorithms or programs to encrypt or encode client information, data, or files without the permission of an authorized supervisor and without taking appropriate measures to ensure that the Company will be able to access the encrypted information;

(ix) Usage of systems for purposes that could directly and/or indirectly cause a strain on any of the computing Systems or prevent/interfere with another person's usage of the Systems. Such uses, include without limitation:

(a) Sending attachments/files that exceed 4mb. to multiple recipients that are not relevant to the business of the Company

(b) spamming

(c) letter bombing

(x) Sending chain letters or messages, whether or not the letters or messages solicit money or goods

(xi) Sending or posting messages which imply or state that the views of the individual user represent the views of the Company, absent appropriate permission from an authorized member of management;

(xii) Viewing or transferring frivolous material or any material not appropriate for business purposes

(xiii) Playing any computer games using Company computer equipment, including shareware.

(xiv) Allowing other persons to access Company Systems, or to use the Employee's user ID or passwords

(xv) Unauthorised posting of any material on the World Wide Web, Usenet (newsgroups), bulletin boards, Internet Relay Chat, or other public forums;

(xvi) Any use of Company computers, computer networks, or other communications systems which is in violation of any applicable local law including, but not limited to, the use of such systems for hacking, cracking, bugging, virus distribution, or accessing and/or tampering with government or private data without authorization;

(xvii) Undermining or ignoring security devices and procedures, including proper use of passwords, firewalls, virus protection software and other devices or procedures that may be installed or instituted in the future;

(xviii) Use of Company computers, computer networks, and/or other communications systems in any manner which violates any applicable ethical rules to which employees of the Company are subject;

(xix) Sending any messages or data in a manner which violates the copyright, patent, trade secret, or other intellectual property laws of India;

(xx) Engaging in any other activity deemed by Company to be in conflict with the intent of this Agreement.

(xxi) Users must not defeat or attempt to defeat any IT System's security – for example, by "cracking" or guessing and applying the identification or password of another User.

Reporting Observed Violations.

If an individual has observed or otherwise is aware of a violation of this Policy, but has not been harmed by the alleged violation, he or she may report any evidence to the Systems Authority overseeing the facility most directly involved, or to the University Information Security Office, which must investigate the allegation and (if appropriate) refer the matter to University disciplinary and/or law enforcement authorities.

Penalties. Individuals found to have violated this Policy may be subject to penalties provided for in other University policies dealing with the underlying conduct. Violators may also face IT-specific penalties, including temporary or

permanent reduction or elimination of some or all IT privileges. The appropriate penalties shall be determined by the applicable disciplinary authority in consultation with the Systems Administrator.

Legal Liability for Unlawful Use. In addition to University discipline, Users may be subject to criminal prosecution, civil liability, or both for unlawful use of any IT System.

ERP Usage Policy

Purpose:

To ensure proper usage of SMUERP and data processed, stored, maintained, or transmitted through it. This includes protection from unauthorized modification, destruction, or disclosure, whether intentional or accidental. This policy is intended to serve as a general overview on SMUERP usage.

Features offered:

Management level: SMUERP provide managers with the information and applications they need to improve operations of the university, hospital, pharmacy etc efficiently.

Employee level: SMUERP provides employees with the information, tools, and services they need to do their jobs, manage their own important work events, and focus on contributing to business results through the their portals.

Employees interaction: SMUERP provides a spontaneous interface with interaction functions that speed up processing and resolution of queries.

General policies:

Users should not attempt to access confidential or proprietary data of the university on SMUERP, except when it is in keeping with the specific assigned duties.

Users should appropriately maintain and protect the confidentiality of any data to which access has been granted.

Users should not make any unauthorized alterations to any data which is accessible either through legitimate granted access or any incidental access.

Remotely or physically logging into or attempting to log into another user's account or attempt to access another user's account, be it for any official use, without the account holder's permission is strictly prohibited.

Workshops and CMEs

As per the requirement of various departments we conduct workshop on the use of SMUERP for new joined employees or existing one on request. This is a regular practice which this department conducts regularly.

We had successfully conducted a 15 days' workshop for **Indo Tibetian border Police**(ITBP) on computer, Internet and Network use for 40 candidates.

We had conducted a one month workshop for **Indo Tibetian border Police**(ITBP) on the topic Hardware and network hands on for 3 candidates .

For various CMEs conducted by other departments as per the request we do help them in providing a general awareness through SMUERP.

Conclusion

This policy cannot and does not cover or describe every situation which may arise with respect to Company computers and communications systems. Therefore, all users are encouraged to carefully consider the actions they take using Company computers and communications systems,