

SIKKIM MANIPAL UNIVERSITY



IT SECURITY POLICIES

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

IMPLEMENTATION DATE – 01/08/2019

REVISION DATE – 01/07/2022



INDEX

Sl. No	Policies
1.	Access Control Policy
2.	IT Asset Management Policy
3.	Information Security Policy
4.	IT Operations Security Policy
5.	Information Security Incident Management Policy
6.	Organisation Information Security Policy
7.	Information Communication Security Policy
8.	Compliance Policy
9.	Human Resource Security Policy
10.	Secure Information Systems Development and Maintenance Policy
11.	Service Vendor Management Policy
12.	Physical Environment Security Policy
13.	Business Continuity Management Policy
14.	Cryptography Policy
15.	E Waste Policy
16.	Email Use Policy
17.	Acceptable Use of IT Resources Policy



Access Control Policy

SMU-ISMS


Version 1.1

(SMU, SMIMS, CRH, SMCPT, SMCON, SMIT)



Revision History

S. No.	Ver. No.	Release Date	Prepared by	Reviewed by	Approved by	Reasons for New Release
1	V1.0	01-08-2019	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) MD Venkatesh Vice Chancellor, SMU	ISMS Implementation
2	V1.1	01-07-2022	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) Rajan S Grewal Vice Chancellor, SMU	Periodic Review


Head IT (SMU)
Prepared by
SIKKIM MANIPAL UNIVERSITY
5th Mile, Tadong
Gangtok, Sikkim
Sikkim Manipal University
737102


Registrar (SMU)
Reviewed by
REGISTRAR
SIKKIM MANIPAL UNIVERSITY
5TH MILE TADONG
SIKKIM 737102



Vice Chancellor (SMU)
Approved by
Dr. (Lt. General) Rajan S. Grewal, AVS
Vice Chancellor (SMU)
Sikkim Manipal University
Tadong, Gangtok (Sikkim)



Table of Contents

1. Introduction	4
2. Abbreviations	4
3. Purpose	4
4. Scope	4
5. Roles & Responsibilities	5
6. Policy Description.....	5
7. Enforcement	9

1. Introduction

This policy defines the controls that need to be implemented and maintained to protect information and information assets of Sikkim Manipal University & its constituents against unauthorized access that poses substantial risk to the organization.

2. Abbreviations

Abbreviations	Description
AAA	Authentication, Authorization and Accountability
AD	Active Directory
Security Admin	Security Administrator
SMU	SMU, SMIMS, CRH, SMCPT, SMCON, SMIT, SMUDDE
MDM	Mobile Device Management

3. Purpose

The purpose of this policy is to define the controls to:

- Restrict access to information and information assets as per University, Institutions requirements.
- Prevent unauthorized access to information IT assets including systems, network services, operating systems and information held in databases and application systems.

4. Scope

- This policy is applicable to all IT Assets of University/Institution. An information asset is a definable piece of information stored, transmitted and/ or processed in any manner, which is recognised as value to the Institution. The types of information assets could be software, physical, paper, service, people, and information that is physically or electronically stored and/ or transmitted by any of the aforesaid types of assets.
- All employees including Faculties / Non-teaching staff, outsourced manpower and third parties of SMU must adhere to this policy in conjunction with all other policies of SMU.

5. Roles & Responsibilities

- The owners of this policy is Head – IT.
- He shall be responsible for the maintenance and updating of this policy document.

Role	Responsibilities
Head – IT	Creation and update of this policy as per requirement
Registrar (SMU)	Review & Approval of this document

6. Policy Description

Access to the information assets of Sikkim Manipal University & its constituents shall be controlled based on institutions and security requirements. Privileges granted shall be based on ‘need-to-know’ and ‘need-to-perform’ criteria.

User Access Management

- A user registration and de-registration process, including seeking appropriate approvals, shall be defined for granting employee /Staff access to any information systems at Institution.
- Access control shall be determined by the Institutes requirements and security classification of information assets and resources to which access is required.
- Access privileges shall be assigned to a unique user ID (AD/Employee ID etc.) that is mapped to an employee based on the employee's role and responsibility.
- Audit trails for all requests for additions, modifications or deletions of user accounts/IDs and access rights shall be maintained and
- An annual review of the access privileges granted to user accounts/ID shall be carried out to identify and facilitate removal/deactivation of inactive accounts.

User Responsibilities for Access Management

- Employees shall be required to maintain a clear desk and lock the screens of their systems prior to leaving them unattended.
- Employees shall set strong alphanumeric passwords and refrain from sharing them by any means
- Employees shall change their passwords on a periodic basis or as per system settings or if there is an indication of a possible compromise of the systems or passwords.



- Passwords for privileged accounts such as system administrator shall be changed once a year, whereas normal user passwords shall be changed every 90 days
- Employees or other third parties shall notify Head IT or Security Administrator or itsupport@smu.edu.in in case of any security breach.

Clear Desk & Clear Screen Policy

- Users shall "log off" or "lock" their computers when their workspace is unattended.
- Users should "shut down" their desktop computers at the end of the workday.
- All 'Highly Restricted' and/or 'Confidential' information in printed form/hard copy shall be removed from the desk and locked in a drawer or file cabinet when the workstation is unattended and at the end of the workday.
- File cabinets containing 'Highly Restricted' and/or 'Confidential' information shall be locked when not in use or when not attended.
- Keys used to access 'Highly Restricted' and/or 'Confidential' information shall not be left at an unattended work area.
- Passwords shall not be posted on or under a computer or in any other accessible location.
- Documents containing Highly Restricted, Confidential or Internal use information must be immediately removed from printers, photocopiers.

Unattended User Equipment

All employees and third parties of the Institutes having access to the information systems shall be required to:

- Terminate active sessions when finished or implement.
- Logout from the workstation, servers and/or network devices when session is over.
- Keep laptops and other mobile devices securely in public areas or in office, if away for a long period.

Network Access Control

- Appropriate interfaces shall be created to segregate the network of SMU from the networks owned by other organization and public networks.
- Appropriate controls for user authentication and access to the network, network services and information systems shall be applied to the SMU network.
- Users shall only be provided with access to the services that they have been specifically authorized to use.



- Authorized users shall be permitted to establish remote connections to SMU network using secure channels.
- A unique identifier for all equipment within the network shall assigned and the same to be used to authenticate all equipment connecting to the network at SMU.
- The network at SMU shall be divided into separate logical network domains. Each network domain shall be protected by appropriate logical security controls.
- For shared networks, especially those extending across the boundaries of SMU, the capability of users to connect to the network shall be restricted, in line with the requirements of university applications.
- Only file transfer applications that encrypt the communication channel shall be used to download or upload files to known secure entities on the internet subject to need based approval.
- Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications
- The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled and monitored.
- External use of remote-access software must be limited to authorized technical support employees
- User sessions shall be managed so as to limit the connection time to sensitive information systems and applications. Additionally, sessions shall be disabled after completion of activity, unless defined otherwise based on system limitations.

Operating System Access Control

- Appropriate logical access to the operating system shall be restricted to authorized users only
- Operating system of servers, workstations and/or network devices shall be controlled through a log-on procedure. The log-on procedure shall not disclose any information of the system. The remote log-on procedure shall be designed with consideration of encryption of information during its transmission
- All employees, contractors, suppliers, vendors and/or third parties of SMU/ Institutions having access to the information systems shall be issued a unique log-in identifier which is not sharable / transferable to the other person.
- An authentication system such as AD shall be implemented to authenticate users.
- Wherever required, additional authentication mechanisms such as tokens, two factor authentication, smart cards etc. should be used.



- Information systems and applications that are accessed from external networks and internet shall be equipped with session time-out control to clear the session screen and terminate both the application and network sessions after completion of activity, unless defined otherwise based on system limitations.

Application and Information Access Control

- Appropriate logical access to the application software shall be restricted to authorized users.
- Access to information and application system functions (menu tabs, access rights or similar) by users and support personnel shall be restricted

Mobile Computing & Communication

- Employees shall be allowed to remotely connect to the network using mobile computing device to access official information, only after successful identification and authentication.
- Employees shall be required to take special care of the mobile computing devices such as laptops, smart devices, mobile phones to prevent compromise and/or destruction of university information.
- Latest virus definitions shall be regularly updated on company provided laptops and desktops to prevent corruption of official data.
- Adequate firewall and/or MDM solution shall be implemented on mobile devices with appropriate SMU policies implemented on them
- Third Party staff shall not connect their mobile computing devices to wired or wireless network of Institute, unless explicitly authorized by appropriate authority (SMU).

Remote Working

Adequate Remote working security measures shall be established and implemented, including:

- Establishing a secure communication channel between teleworkers and network of Institution.
- Use of appropriate authentication mechanism for authenticating those using teleworking solutions
- Revocation of authority, access rights and return of equipment when teleworking activity ceases or when the employee exits from Institute.



Physical Access control to Server Rooms and other Facilities

- Data Centre/Server Room and all critical data points shall be physically secured, to prevent a break-in/unauthorized entry.
- Entry into the data centres/server rooms shall be restricted to authorized personnel only with approvals of respective Function Heads who shall do the necessary verification/diligence checks.
- Entry to data centre / Server room for external vendors who require to work on the maintenance or repair of the equipment of data centre shall be allowed in with escort, throughout their stay, by the physical security staff or respective activity owner.
- Secure authentication through biometric reader shall be installed at all critical entry points such controller examination office etc.
- CCTVs and alarms shall be set up at all data centres/server rooms
- CCTV/Biometric access shall be monitored, and recordings/logs reviewed weekly for any alerts and maintained for a minimum of 10 days
- In the absence of CCTV surveillance, a security person should be deployed at the entrance of the Data Centre / Server Room
- A register to record and monitor entry and exit to and from the data centre / server room shall be maintained by the Security personnel
- Data centre/server room access control system and doors shall be designed to operate in case of utility power outage as well as biometric application/hardware failure
- Management of security alarms, CCTV systems and visitor book details shall be restricted to security staff and Facilities staff only
- A yearly reconciliation of physical access rights to the data centres/server rooms shall be conducted and any discrepancies shall be communicated to the respective functions for further appropriate action

7. Enforcement

This policy will be reviewed and revised from time-to-time based on business and (or) technological requirements and the same shall be published as revised versions. Any deviation from the above policy should be documented, approved and signed by Head IT.

-----End of Document-----



IT Asset Management Policy


SMU-ISMS Version - 1.1

(SMU, SMIMS, CRH, SMCPT, SMCON, SMIT)



Revision History

S. No.	Ver. No.	Release Date	Prepared by	Reviewed by	Approved by	Reasons for New Release
1	V1.0	01-08-2019	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) MD Venkatesh Vice Chancellor, SMU	ISMS Implementation
2	V1.1	01-07-2022	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) Rajan S Grewal Vice Chancellor, SMU	Periodic Review


Head IT (SMU)
Prepared by
HEAD -IT
SIKKIM MANIPAL UNIVERSITY
5th Mile, Tadong
Gangtok, Sikkim
Sikkim Manipal University
737102


Registrar (SMU)
Reviewed by
REGISTRAR
SIKKIM MANIPAL UNIVERSITY
5TH MILE TADONG
SIKKIM 737102


Vice Chancellor (SMU)
Approved by
Dr. (Lt. General) Rajan S. Grewal, AVS, IAS
Vice Chancellor (SMU)
Sikkim Manipal University
Tadong, Gangtok (Sikkim)



Contents

1. Introduction	4
2. Abbreviations	4
3. Purpose	4
4. Scope	5
5. Roles & Responsibilities	5
6. Policy Description	5
7. Related Policies/Processes	8

1. Introduction

Information assets created, received, or distributed by the employees of Sikkim Manipal University & its constituents need to be protected against threats. This necessitates identification of information asset, asset owner, asset custodian, asset classification and determining confidentiality, integrity and availability ratings of the asset and then finally computing the asset value. Additionally, they need to be classified and labelled according to predefined levels of criticality and sensitivity. Safeguards and controls need to be designed to protect information assets from unauthorized access, distribution, destruction or disclosure.

2. Abbreviations

Abbreviations	Description
A	Availability
C	Confidentiality
Security Admin	Security Administration
I	Integrity
ICT	Information and Communication Technology
IP	Intellectual Property
SMU	SMU, SMIMS, CRH, SMCOP, SMCON, SMIT, SMUDE
PII	Personally, Identifiable Information
SBI	Sensitive University Information
SPI	Sensitive Personal Information

3. Purpose

The purpose of this policy is to ensure:

- An Information Asset Register documenting types of information assets of each University function is maintained.

- The information assets of each business function have designated owners and custodians.
- All information assets are identified and appropriately labelled.
- These information assets are handled by authorized persons in a manner that ensures their protection.

4. Scope

- This policy is applicable to all information assets of Sikkim Manipal University & its constituents . An information asset is a definable piece of information stored, transmitted and/ or processed in any manner, which is recognised as value to the Institute. The types of information assets could be software, physical, paper, service, people and information that is physically or electronically stored and/ or transmitted by any of the aforesaid types of assets.
- All employees including teaching / non-teaching staff, outsourced and third party's role of SMU must adhere to this policy in conjunction with all other policies of SMU-ISMS.

5. Roles & Responsibilities

The owner of this policy is the Head IT, He shall be responsible for the maintenance and updating of this policy document.

Role	Responsibilities
Asset Owner	The Head of a Function is generally considered to be an Asset Owner. He/she is responsible for the identification, classification and rating of the assets that are being used/managed in the function and further to ensure that Asset Custodians implement appropriate controls for the protection of the asset.
Asset Custodian	An Asset Custodian is the person responsible for day-to-day operations/maintenance of assets. He/she should manage the entire asset lifecycle.
Head IT	Creation and update of this policy as per requirement
Registrar (SMU)	Review & Approval of this document

6. Policy Description

Information assets of SMU shall receive comprehensive protection and shall have an identified Asset Owner and Asset Custodian, also have appropriate labelling and handling mechanisms.

Information Asset Register

The IT Asset Register documents the information assets of a function. All functions are required to maintain such a register. The Information Asset Register is required to contain, at a minimum, the following information about the assets:

- Name of the function that uses this asset
- The Name, Type (Hardware, Software, Information, Infrastructure, People), Description and Location of the asset.
- The Asset Owner and Asset Custodian.
- The C, I, A ratings of the asset. (C- Confidentiality, I- Integrity, A- Availability)
- The Asset Value computed as the product of the C, I, A values.

Ownership of Information Assets

The Asset Owner is required to ensure that he/she discharges the responsibilities as described in the *Roles & Responsibilities* section above.

Further, he/she shall periodically check to ensure that information assets continue to be classified appropriately and that the safeguards remain valid and operative.

Information Classification

The information classification categories shall be used to define an appropriate level of protection or special handling needed for the information asset. The classification of the information needs to be consistent with the University requirement and considers 'Confidentiality', 'Integrity' and 'Availability' ratings of the information. The classification is done as per the table below:

Classification Level	Types of Information Assets	Examples
Highly Restricted	Personally, Identifiable Information (PII), Sensitive Personal Information (SPI), Intellectual Property (IP), Sensitive University Information (SBI)	PII - Name, Address, Phone number etc., SPI - Health Records, Biometric Records etc., SBI - Trade secrets, Acquisition plans, Financial data
Confidential	On need to know basis only, for named Employees/Customers/Vendors/Contractors etc. (applicable to both Internal and External Information)	Agreements, Contracts, Purchase Orders etc.
Internal	Information meant to be used/circulated within the Organization	ISMS, Applications to be used by employees etc.



Public	Any information that can be shared with everyone	Certifications, Affiliations, Achievements, Organization website etc.
---------------	--	---

Information Asset Labelling

All information assets should be labelled. The asset owners are required to ensure that their assets are appropriately labelled for ease of identification. Refer *Information Asset Management Process* for details of the methods used for asset labelling and handling.

Acceptable Use of Information Assets

All information assets shall be limited to University purposes only. SMU (IT) reserves the right to monitor and report this usage (please refer *Information Security Incident Management Policy*).

The following are deemed unacceptable uses of information assets of SMU and its colleges.:

- Transmitting, modifying or otherwise removing information from the office for personal/ malicious use, that contravenes the privacy of customers and SMU personnel and SMU intellectual property.
- Wasting computer resources or monopolizing those resources to the exclusion of other users
- Propagating malware
- Engaging in activities that disrupt network communications and/or system availability
- Circumventing user authentication or authorization on any system
- Installing and/or using unlicensed or non-approved software, data and hardware.
- Connecting any hardware that is unapproved, to the network of SMU colleges and
- Other activities that are deemed unacceptable by the HR, Facilities or other function and that are illegal

Further:

- Only information assets (e.g. desktops, laptops, or any other ICT device) managed or approved by SMU shall be used to store, transmit and/or connect to the institute's internal network
- Formal approval should be obtained from Head IT and/or Registrar (SMU) before any information assets that are not managed by SMU are used to connect to the network
- Where approval has been obtained, any information assets that are not managed by SMU (IT) (e.g. personal devices such as smart devices, tablets etc.) are used to connect to the Institute's network, is subject to SMU'S IT security requirements set out for:
 - viruses and other malware
 - ICT devices
 - wireless networks

- remote access and
- messaging and internet use
- Prior to information being taken away from the office, the following should be considered:
 - sensitivity of the information.
 - potential impact of loss or disclosure of the information and
 - precautions that need to be taken to avoid loss or disclosure.
- Encryption or an equivalent method of protection should be used to secure sensitive information of SMU Colleges when:
 - Transmitted over non-corporate networks such as the internet and social media platforms and
 - Stored on ICT devices and removable media

Information Asset Retention and Disposal

All information assets classified as Highly Restricted, Confidential, Internal or Public should be provided with a retention timeframe.

The retention schedules are defined by the Asset Owners. The assets are retained as follows:

- Information in electronic format must be stored in an encrypted format and/or must be protected with strong passwords.
- Information assets such as documents and records, which are present in a physical format, must be stored only in locked drawer or cabin.
- Information must be disposed when no longer needed subject to its retention schedule. Approval of Asset Owner is required if information is disposed by a person other than the Asset Owner.
- Physical and electronic copies should be stored and disposed as per the *Information Asset Management Process*.

7. Related Policies/Processes

- Information Asset Management Process
- Cryptography Policy
- Information Security Incident Management Policy
- Organisation of Information Security Policy

-----End of Document-----



Information Security Policy


SMU-ISMS Version - 1.1

(SMU, SMIMS, CRH, SMCPT, SMCON, SMIT)



Revision History

S. No.	Ver. No.	Release Date	Prepared by	Reviewed by	Approved by	Reasons for New Release
1	V1.0	01-08-2019	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) MD Venkatesh Vice Chancellor, SMU	ISMS Implementation
2	V1.1	01-07-2022	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) Rajan S Grewal Vice Chancellor, SMU	Periodic Review


Head IT (SMU)
Prepared by
SIKKIM MANIPAL UNIVERSITY
5th Mile, Tadong
Gangtok, Sikkim
Sikkim Manipal University
737102


Registrar (SMU)
Reviewed by
REGISTRAR
SIKKIM MANIPAL UNIVERSITY
5TH MILE TADONG
SIKKIM 737102



Vice-Chancellor (SMU)
Approved by
Dr. (Lt. General) Rajan S. Grewal, AVS, IFSM
Vice Chancellor (SMU)
Sikkim Manipal University
Tadong, Gangtok (Sikkim)



Table of Contents

1. Introduction	4
2. Abbreviations	4
3. Purpose	4
4. Scope	4
5. Roles & Responsibilities	5
6. Policy Description	5
7. Enforcement	6

1. Introduction

The policy defines that IT assets are provided comprehensive protection against the consequence of breaches of confidentiality, failure of integrity and/or interruptions to their availability. The Sikkim Manipal University’s Information Security Policy provides management, the direction and support to implement information security across the organisation.

2. Abbreviations

Abbreviations	Description
SMU	SMU, SMIMS, CRH, SMCPT, SMCON, SMIT, SMUDEDE
ISMS	Information Security Management System

3. Purpose

The purpose of the Information Security Policy is to ensure the business continuity of SMU and its constituents to minimize the risk of damage by preventing security incidents and reducing their potential impact.

4. Scope

- The SMU Information Security Policy is applicable to all information assets of SMU. An information asset is a definable piece of information stored, transmitted and/ or processed in any manner, which is recognised as value to the University. The types of information assets could be software, physical, paper, service, people and information that is physically or electronically stored and/ or transmitted by any of the aforesaid types of assets.
- All employees and third parties of SMU must adhere to this policy in conjunction with all other policies of SMU. Anyone having questions regarding this policy shall consult with the SMU Information Security core team.

5. Roles & Responsibilities

The owner of this policy is the Head IT. He shall be responsible for the maintenance and updating of this policy document.

Role	Responsibilities
Head IT	Creation and update of this policy as per requirement
Registrar (SMU)	Review and Approval of this document

6. Policy Description

Policy Objective

The objective of information security is to ensure the business continuity of SMU and to minimize the risk of damage by preventing security incidents and reducing their potential impact.

Policy Statement

SMU Information Security Policy aims to protect the information assets of SMU against all internal and external threats.

The security policy ensures that:

- Information is protected against unauthorized access.
- Confidentiality of information is ensured.
- Integrity of information is maintained.
- Availability of information for University processes is ensured.
- Legislative and regulatory requirements are met.
- Information Security risks are identified and managed in accordance with the framework defined by SMU.
- University continuity plans are developed, maintained and tested, as applicable.
- Periodic Information security training and awareness is conducted for all employees.

- All actual or suspected information security breaches are reported and managed in accordance with the defined incident management framework.

The Vice Chancellor of the University has approved the information security policy. The Head IT is responsible for maintaining the policy and providing support and advice during its implementation. Associated policies as well as processes exist to support this policy.

This policy and its supporting policies shall be reviewed by Management for suitability to the organization at least once a year.

This policy allows users to access information and essential services when needed. All Heads OF respective functions are directly responsible for implementing this policy and ensuring staff compliance in their respective functions. Compliance with the Information Security Policy is mandatory.

7. Enforcement

This policy will be reviewed and revised from time-to-time based on business and (or) technological requirements and the same shall be published as revised versions. Any deviation from the above policy should be documented, approved and signed by Head IT.

Related Policies

- Access Control Policy
- Information Asset Management Policy
- Business Continuity Management Policy
- Communications Security Policy
- Cryptography Policy
- Human Resource Security Policy
- Information Security Incident Policy
- Secure Information System Development and Maintenance Policy
- Operations Security Policy
- Organisation of Information Security Policy

-----End of Document-----



IT Operations Security Policy

SMU-ISMS


Version - 1.1

(SMU, SMIMS, CRH, SMCPT, SMCON, SMIT)



Revision History

S. No.	Ver. No.	Release Date	Prepared by	Reviewed by	Approved by	Reasons for New Release
1	V1.0	01-08-2019	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) MD Venkatesh Vice Chancellor, SMU	ISMS Implementation
2	V1.1	01-07-2022	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) Rajan S Grewal Vice Chancellor, SMU	Periodic Review


Head IT (SMU)
Prepared by
SIKKIM MANIPAL UNIVERSITY
5th Mile, Tadong
Gangtok, Sikkim
Sikkim Manipal University
737102


Registrar (SMU)
Reviewed by
REGISTRAR
SIKKIM MANIPAL UNIVERSITY
5TH MILE TADONG
SIKKIM 737102



Vice Chancellor (SMU)
Approved by
Dr. (Lt General) Rajan S. Grewal, AVS
Vice Chancellor (SMU)
Sikkim Manipal University
Tadong, Gangtok (Sikkim)

Table of Contents

1. Introduction.....	4
2. Abbreviations.....	4
3. Purpose.....	4
4. Scope	4
5. Roles & Responsibilities	5
6. Policy Description	5
7. Enforcement	9

1. Introduction

The IT Operations Security Policy is designed to ensure appropriate security controls such as, but not limited to documented operating procedures, data backup, protection against malicious code, secure exchange of information, etc. are implemented for the hardware and software assets of Sikkim Manipal University & its constituents to prevent unauthorized access to, misuse or failure of systems so as to ensure confidentiality, integrity and availability of information.

2. Abbreviations

Abbreviations	Description
SMU	SMU, SMIMS, CRH, SMCPT, SMCON, SMIT, SMUDDE
ISMS	Information Security Management System

3. Purpose

The purpose of this policy is to define and implement appropriate controls to prevent unauthorized access to, misuse or failure of various systems so as to ensure confidentiality, integrity and availability of information.

4. Scope

- This policy is applicable to all information assets of SMU. An information asset is a definable piece of information stored, transmitted and/ or processed in any manner, which is recognised as value to the University. The types of information assets could be hardware, software, physical, paper, service, people and information that is physically or electronically stored and/ or transmitted by any of the aforesaid types of assets.
- All employees and third parties of SMU must adhere to this policy in conjunction with all other policies of SMU.

5. Roles & Responsibilities

The owner of this policy is the Head IT. He shall be responsible for the maintenance and updating of this policy document.

Role	Responsibilities
Head of IT	Creation and update of this policy document
Registrar ,SMU	Review and Approval of this document

6. Policy Description

SMU shall ensure effective and secure operations of its information systems. Appropriate controls shall be implemented to protect the information contained in, transmitted by and/or processed by these information systems and ensure their uninterrupted operation.

Operating Procedures

- Standard Operating Procedures and responsibilities for all SMU information processing facilities shall be formally authorized, documented, maintained and reviewed annually.
- SOPs could include those pertaining to, but not limited to, email, firewall or server configuration; hardware and other equipment etc.
- Changes to the SOPs shall be carried out as per the change management process.

Change Management

- Change Management shall be implemented in order to be applicable to any change that could impact confidentiality, integrity or availability of information processed by or stored in the information systems. This shall, at a minimum, include the following:
 - Assessment of potential impact, including security impact
 - Identification of person authorizing change
 - Formal approval process for proposed changes
 - Procedures for testing, including security testing of the changes
 - Communication of details of changes to all affected parties
 - Recording of all changes
 - Roll-back procedures for aborting or recovering from failed changes
- Changes to any system shall be monitored for compliance with established process
- Change controls shall be applied to all security related aspects of SMU production environment

- All approved changes to the critical systems shall be tested prior to implementation
- All third-party service providers shall follow change management as described above.

Separation of development, test, and operational facilities

- Appropriate security controls shall be identified and implemented to ensure logical separation between development, test and production environments.

Protection against Malware

- IT shall manage Endpoint Security
- Antivirus administration shall be managed through a centralized system
- Further, IT shall manage controlling of the updates, reporting and monitoring to all the endpoints from the centralized antivirus management console.
- Online antivirus scan shall be configured on desktops, laptops and servers in SMU
- All desktops and laptops shall have advanced threat protection enabled to protect from malicious traffic
- Advance threat management system must be configured to monitor any non-updated clients and virus outbreaks/infection alerts on daily basis.
- If any vulnerability is found within the network, an alert shall be immediately generated by the Antivirus server and suitable action shall be initiated on priority to fix the same if not resolved by Antivirus Signatures
- Status report shall be generated on a weekly basis.
- Antivirus signature update in all SMU systems shall not be older than one day when in the network or online
- Proper analysis shall be performed of residual virus/malware, antivirus-specific issues on systems to ensure vulnerability-free SMU environment
- For SMU email servers, virus detection and attachment filtering shall be enabled.
- DLP (Data Leakage Prevention) controls shall be implemented. On end user systems based on University needs.
- By default, all servers, desktops and laptops are installed with the latest, updated antivirus agent at the time of the asset commissioning or allocation to users
- Users shall not have any access to modify the antivirus agent configuration on their systems.

Restrictions on software installation

- Only authorized software shall be allowed for installation on SMU systems as this shall ensure in reducing the risk of malware
- Freeware/Shareware shall not be installed inside the SMU network. Approvals for exceptions for freeware / shareware installations need to be taken specifically for University requirement
- IT shall perform vulnerability scan and obtain official clearance for any freeware and shareware installation
- All software installation inclusive of updates and security patches to existing software shall be installed post testing
- Any University user who has requested for a software installation due to University requirement, shall get a written approval from respective manager.
- Downloading unlicensed software/utility, freeware, games, movies, music, etc. shall be strictly prohibited on the SMU network.
- Audit or maintenance activities of servers and other critical systems shall be carefully planned and agreed to minimize disruptions to University processes.

Vulnerability Management

- Vulnerability assessments shall be performed periodically on University-critical information assets for vulnerabilities.
- All identified high and medium severity vulnerabilities shall be addressed within 30 to 90 days respectively, from the date of being reported.

Patch Management

- All servers shall be regularly updated with the latest patches as per the patch calendar
- All desktops and laptops shall be deployed with baseline patches while allocating the assets to users
- A rollback plan shall be in place that allows safe restoration of critical systems to their pre-patch state in the event that the applied patch has unforeseen effects.

Log Management

- Log Management shall ensure that a defined process exists for management of University-critical information systems and devices logs.

- All access control devices, critical servers, networking devices and other security devices shall generate access, usage and configuration change logs
- System administrator and operator activities shall also be logged
- Audit logs shall be analyzed periodically for any deviation from the baseline and for suspected/malicious activities
- Audit logs for System Administrator or third-party access need to be reviewed on periodic basis
- The log storage, retention and disposal shall be performed as per the contractual requirements
- Audit logs shall be archived to collect any evidence and shall be protected from any possible tampering
- Access to the log files shall be restricted.

Data Backup Policy

- Data on servers/applications shall be backed up as per the schedule defined and approved by IT team
- Backup frequencies, scope of coverage, choice of media shall be defined and approved by IT in agreement with the respective asset owner.
- Where necessary, additional copies of backup data shall be stored at a remote site for contingency purposes
- The backed-up data shall be periodically tested for successful restoration and functionality.
- Backup logs generated from each backup job shall be reviewed for errors.
- Backup mechanism must be auto defined and restoration must be check on regularly.

Clock Synchronization

- All clocks of SMU, including those of servers, desktops, laptops and other devices shall be synchronized with a Network Time Protocol (NTP) server or equivalent.

7 Enforcement

This policy will be reviewed and revised from time-to-time based on business and (or) technological requirements and the same shall be published as revised versions. Any deviation from the above policy should be documented, approved and signed by Head IT.

Related Policies

- Access Control Policy
- Communication Security Policy
- Cryptography Policy
- Information Security Incident Management Policy

-----End of Document-----

Information Security Incident Management Policy

SMU-ISMS


Version 1.1

(SMU, SMIMS, CRH, SMCPT, SMCON, SMIT)



Revision History

S. No.	Ver. No.	Release Date	Prepared by	Reviewed by	Approved by	Reasons for New Release
1	V1.0	01-08-2019	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) MD Venkatesh Vice Chancellor, SMU	ISMS Implementation
2	V1.1	01-07-2022	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) Rajan S Grewal Vice Chancellor, SMU	Periodic Review


Head IT (SMU)
Prepared by
SIKKIM MANIPAL UNIVERSITY
5th Mile, Tadong
Gangtok, Sikkim
Sikkim Manipal University
737102


Registrar (SMU)
Reviewed by
REGISTRAR
SIKKIM MANIPAL UNIVERSITY
5TH MILE TADONG
SIKKIM 737102



Vice Chancellor (SMU)
Approved by
SIKKIM MANIPAL UNIVERSITY
5TH MILE TADONG
SIKKIM 737102

Table of Contents

1. Introduction	4
2. Abbreviations	4
3. Purpose	4
4. Scope	4
5. Roles & Responsibilities	5
6. Policy Description	5
7. Enforcement.....	6

1. Introduction

Information Security Incident management involves the identification, reporting and mitigation of information security incidents and further, to take actions to avoid any future recurrence.

2. Abbreviations

Abbreviations	Description
SMU	SMU, SMIMS, CRH, SMCPT, SMCON, SMIT
IRT	Incident Response Team
ISMS	Information Security Management System
RCA	Root Cause Analysis

3. Purpose

The purpose of this policy is to establish an effective Information Security Incident Management system at SMU to minimize the damage due to information security incidents and malfunctions.

4. Scope

- This policy is applicable to all information assets of SMU. An information asset is a definable piece of information stored, transmitted and/ or processed in any manner, which is recognised as value to the University. The types of information assets could be software, physical, paper, service, people and information that is physically or electronically stored and/ or transmitted by any of the aforesaid types of assets.
- All employees and third parties of SMU must adhere to this policy in conjunction with all other policies of SMU.

5. Roles & Responsibilities

The owner of this policy is the Head IT (SMU). He shall be responsible for the maintenance and updating of this policy document.

Role	Responsibilities
Head IT (SMUI)	Creation and update of this policy as per requirement
Registrar (SMU)	Review and Approval of this document
IRT	Reporting, recognizing, and resolving information security incidents and weaknesses and oversight for information security incidents

6. Policy Description

A formal information security event/incident detection, reporting and escalation process shall be established. Responsibilities and procedures shall be defined to handle information security events effectively. All employees and third parties of SMU shall be trained on their responsibilities related to incident management.

Information Security Event and Incident

Security violations such as unauthorized physical or logical access to SMU facilities, intrusions, virus attacks, software malfunctions, misuse of IT resources, violation of SMU policies and standards, violation of applicable laws, security weaknesses, and any other occurrence which has, or may have, a negative impact on the confidentiality, integrity, and/or availability of SMU information shall be considered as information security incidents. Every occurrence is an event and it becomes an incident once there is a negative impact on SMU.

Incident Reporting

- Each SMU employee or third party who suspects or learns of a threat or potential incident should immediately report it by logging the same appropriately into SMU Service desk.
- The IRT should follow the *Information Security Incident Management process* for engaging its function.

Incident Response Team (IRT)

- The Head IT shall be the designated primary contact for reporting of information security incidents.

- The Head IT along with the Registrar (SMU) shall identify the Incident Response Team (IRT) and define roles and responsibilities of the IRT members who shall respond to information security incidents
- The roles and responsibilities of the IRT team members include:
 - Reporting, recognizing, and resolving information security incidents and weaknesses and
 - Oversight for information security incidents
- IRT shall contain personnel from cross-functional teams who have the authority to take decisions. Members from one or more of the following teams should be included for handling and resolving incidents:
 - Representative of HOI
 - Finance
 - Human Resource
 - IT
 - Facilities

However, it is at the discretion of the Registrar (SMU) to choose the appropriate team to form the IRT

- *Information Security Incident Management process* with escalation matrices shall be documented and followed for responding to information security incidents.

7. Enforcement

This policy will be reviewed and revised from time-to-time based on business and (or) technological requirements and the same shall be published as revised versions. Any deviation from the above policy should be documented, approved and signed by Head IT.

Related Policies

- Information Asset Management Policy
- Human Resource Security Policy
- Organization of Information Security Policy
- Physical and environmental Security Policy

-----End of Document-----



Organisation Information Security Policy

SMU-ISMS


Version - 1.1

(SMU, SMIMS, CRH, SMCPT, SMCON, SMIT)



Revision History

S. No.	Ver. No.	Release Date	Prepared by	Reviewed by	Approved by	Reasons for New Release
1	V1.0	01-08-2019	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) MD Venkatesh Vice Chancellor, SMU	ISMS Implementation
2	V1.1	01-07-2022	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) Rajan S Grewal Vice Chancellor, SMU	Periodic Review


Head IT (SMU)
Prepared by
SIKKIM MANIPAL UNIVERSITY
5th Mile, Tadong
Gangtok, Sikkim
Sikkim Manipal University
737102


Registrar (SMU)
Reviewed by
REGISTRAR
SIKKIM MANIPAL UNIVERSITY
5TH MILE TADONG
SIKKIM 737102



Vice Chancellor (SMU)
Approved by
Dr. (Lt. General) Rajan S. Grewal, AVS
Vice Chancellor (SMU)
Sikkim Manipal University
Tadong, Gangtok (Sikkim)



Table of Contents

1. Introduction	4
2. Abbreviations	4
3. Purpose	4
4. Scope	4
5. Roles & Responsibilities	5
6. Policy Description	5
7. Enforcement.....	9

1. Introduction

The Information Security Policy Organisation appropriate responsibilities, authority and relationships to manage information security at Sikkim Manipal University and its constituents . The Information Security organization has representation from all functions to ensure the structured coordination of information security related activities within the organisation. This policy addresses the above requirements of the organization.

2. Abbreviations

Abbreviations	Description
ISMS	Information Security Management System
MRM	Management Review Meeting
SMU	SMU, SMIMS, CRH, SMCPT, SMCON, SMIT

3. Purpose

The purpose of this policy is to:

- Define an information security organisation structure to implement, monitor, manage and improve organization wide information security
- Assign appropriate responsibilities, authorities and relationships to manage information security at Sikkim Manipal University.

4. Scope

- This policy is applicable to all information assets of SMU. An information asset is a definable piece of information stored, transmitted and/ or processed in any manner, which is recognised as value to the business. The types of information assets could be software, physical, paper, service, people and information that is
- physically or electronically stored and/ or transmitted by any of the aforesaid types of assets.
- All employees and third parties of University must adhere to this policy in conjunction with all other policies of SMU.

5. Roles & Responsibilities

The owner of this policy is the Head IT. He shall be responsible for the maintenance and updating of this policy document.

Role	Responsibilities
Head IT	Creation and update of this policy as per requirement
Registrar (SMU)	Review and Approval of this document

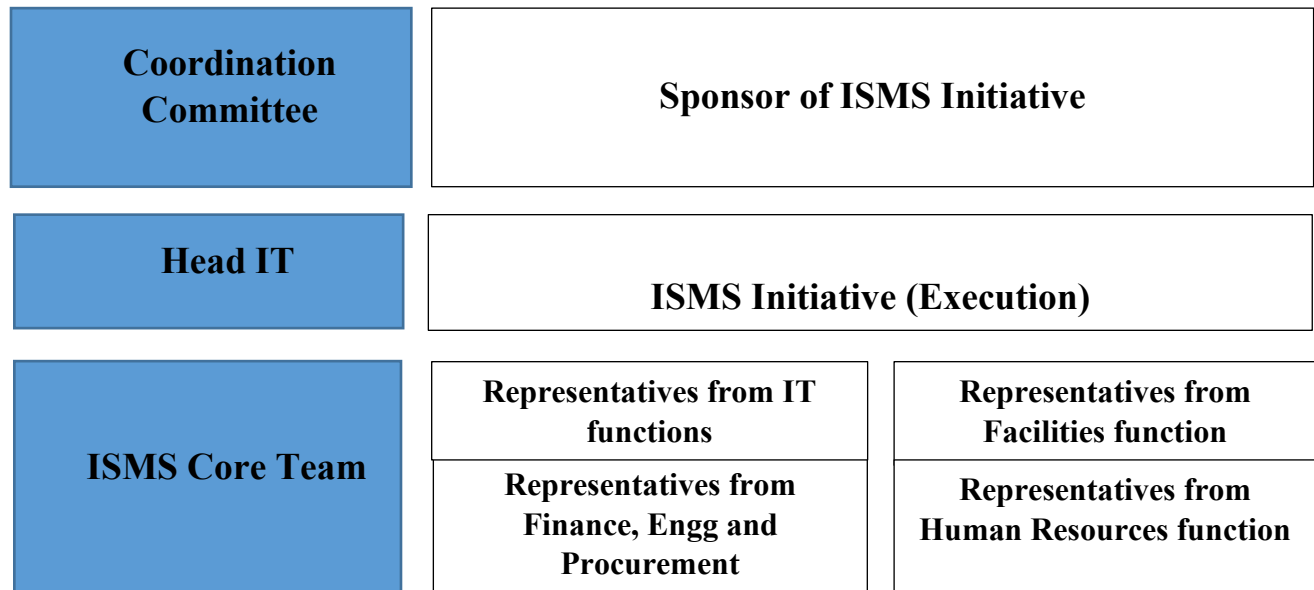
6. Policy Description

- An Information Security Organization shall be setup to undertake information security activities in all functions of SMU.
- An information security organization structure shall be established to implement, monitor, manage and improve the organization wide information security
- Security roles and responsibilities shall be defined and assigned at all levels
- The Information Security Organization structure should be reviewed annually and after any changes in business, regulatory or operational requirements.

Information Security Organization Structure

Given below is the information security organization structure defined for SMU.





Information Security Roles and Responsibilities

➤ Coordination Committee (CC)

The CC provides management commitment, sponsor and support for information security initiatives.

The CC meeting will be held once in a Month.

The CC have the following Role & Responsibilities:

- Reviewing and approving the SMU Information Security Policy as well as other related policies and procedures.
- Providing the resources needed for information security management and approving assignment of specific roles & responsibilities for implementation.
- Communicating to the employees and third- parties on the SMU Information Security Policy and plans to demonstrate management intent.
- Conducting review of security initiatives and plans
- Providing feedback and inputs to enhance the information security of SMU.
- Ensuring conduct of security compliance reviews (including processes and technology) by an independent agency and
- Providing decision on organization's risk appetite (acceptable level of security risk).

➤ **Head Information Technology (Head IT)**

The Head of IT shall have the following responsibilities:

- Identifying information security objectives and aligning them with the organizational strategic plans
- Overseeing the development and implementation of the security initiatives, plans, policies, processes, and their ongoing maintenance
- Ensuring the establishment and implementation of security risk management framework across the enterprise
- Carrying out regular risk assessments across the organization including third- parties and providing the Head IT with a view of risk exposure to seek inputs on risk treatment/acceptance measures
- Overseeing security operations including but not limited to anti-virus management, end point protection, patch management, firewall policy management, vulnerability management, etc.
- Overseeing investigations/forensic analysis of security breaches, including suspected insider threats
- Assisting in incident management associated with security breaches
- Assisting the HR in planning and executing the security awareness programs
- Overseeing the development and implementation of Business Continuity and Disaster Recovery plan, framework and solutions.
- Keeping the management updated with effective and reliable approaches to information security
- Conducting the regular security maturity and compliance reviews including External and Internal Audits across the organization and reporting the outcome to the Vice Chancellor.

➤ **ISMS Core Team**

The ISMS Core Team will have representatives from the following functions:

- Information Technology consisting of –
 - - Vice Chancellor, SMU
 - Head of Institutions
 - Registrar (SMU)
 - Head of Office Operations
 - Head of Finances, HR & General Services
 - Head IT

The ISMS core team shall meet at least once every month. Members of the team would have secondary responsibilities of information security in addition to their existing primary responsibilities.

The ISMS Core Team shall have following information security responsibilities:

- Acting as representatives of their respective function for information security issues pertaining to their function.
- Implementing, within their respective functions, the information security requirements as specified in the ISMS Policy and its domain specific policies.
- Resolving any inter-functional issues that may arise while implementing the security policies in their function.
- Ensuring that the third parties related to their function adhere to the ISMS Policy and its domain specific policies and informing the Head IT in case any non-compliance is observed.
- Creating and maintaining the information asset register for their respective function as per the template provided by the IT.
- Providing inputs/feedback to the HEAD IT to improve the information security at SMU. Assisting the SMU (IT) in carrying out security risk assessments and compliance reviews for their respective function including the associated third parties and
- Providing the SMU (IT) with required data to measure the maturity of ISMS in their respective function.

Contact with Authorities

- The SMU Facilities team shall maintain contact with law enforcement agencies, fire department and emergency services. Contact details of these agencies shall be maintained and displayed at appropriate places that are accessible to all users.
- The SMU Facilities shall ensure the validity and accessibility of the authorities' contact numbers, once in a quarter. This is for preparedness in case of any emergencies.
- The IT Team shall maintain regular contact with telecommunication service providers and other service providers supporting the IT infrastructure and applications.

Contact with Special Interest Groups

The Head IT shall maintain appropriate contact with special interest groups and authorized information security forums for receiving and distributing the updates on new vulnerabilities, security threats, regulations, risks etc. pertaining to SMU.

Third Party Service Providers

- All third -party service providers, contractors and sub-contractors shall be required to adhere to the SMU ISMS policy;
- All third-party service providers, contractors and sub-contractors shall be required to submit specific documents such as Legal and Non-disclosure Agreements etc. pertaining to information security prior to any engagement and
- All third-party service providers, contractors and sub-contractors shall be subject to independent reviews of their compliance with this policy.

7. Enforcement

This policy will be reviewed and revised from time-to-time based on business and (or) technological requirements and the same shall be published as revised versions. Any deviation from the above policy should be documented, approved and signed by Head IT.

Related Policies

- Information Security Policy
- Vendor Management Policy
- Information Security Incident Management Policy

-----End of Document-----



Information Communication Security Policy

SMU-ISMS

Version - 1.1

(SMU, SMIMS, CRH, SMCPT, SMCON, SMIT)



Revision History

S. No.	Ver. No.	Release Date	Prepared by	Reviewed by	Approved by	Reasons for New Release
1	V1.0	01-08-2019	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) MD Venkatesh Vice Chancellor, SMU	ISMS Implementation
2	V1.1	01-07-2022	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) Rajan S Grewal Vice Chancellor, SMU	Periodic Review

Head IT (SMU)

Prepared by

SIKKIM MANIPAL UNIVERSITY
5th Mile, Tadong
Gangtok, Sikkim

SIKKIM MANIPAL UNIVERSITY
5th Mile, Tadong
Gangtok, Sikkim
737102

Registrar (SMU)
Reviewed by
REGISTRAR
SIKKIM MANIPAL UNIVERSITY
5TH MILE TADONG
SIKKIM 737102

Vice Chancellor (SMU)
Approved by
Dr. (Lt. General) Rajan S. Grewal, AVSM, VSM
Vice Chancellor (SMU)
Sikkim Manipal University
Tadong, Gangtok (Sikkim)



Table of Contents

1. Introduction	4
2. Abbreviations	4
3. Purpose	4
4. Scope	4
5. Roles & Responsibilities	5
6. Policy Description	5
7. Enforcement.....	8

1. Introduction

Communications Security aims to ensure appropriate security controls for the protection of information in networks and its supporting information processing facilities to ensure confidentiality, integrity and availability of information residing on the hardware and software assets of Manipal Sikkim Manipal University & its constituents .

2. Abbreviations

Abbreviations	Description
SMU	SMU, SMIMS, CRH, SMCPT, SMCON, SMIT
ISMS	Information Security Management System
LAN	Local Area Network
MPLS	Multi-Protocol Label Switching
SSL	Secure Sockets Layer
VPN	Virtual Private Network

3. Purpose

The purpose of this policy is to define and implement appropriate controls to protect the information stored in or passing over networks and their supporting information processing facilities.

4. Scope

- This policy is applicable to all information assets of SMU. An information asset is a definable piece of information stored, transmitted and/ or processed in any manner, which is recognised as value to the University. The types of information assets could be software, physical, paper, service, people and information that is physically or electronically stored and/ or transmitted by any of the aforesaid types of assets.
- All employees and third parties of SMU must adhere to this policy in conjunction with all other policies of SMU.

5. Roles & Responsibilities

The owner of this policy is the Head IT. He shall be responsible for the maintenance and updating of this policy document.

Role	Responsibilities
Head – IT	Creation and update of this policy document
Registrar (SMU)	Review and Approval of this document

6. Policy Description

This policy intends to implement appropriate security controls to ensure the protection of information in networks and its supporting information processing facilities to ensure confidentiality, integrity and availability of information residing on SMU information systems.

General Guidelines

- All 3RD party connections/VPN connectivity should be segregated from the SMU Network.
- External connections to SMU networks, i.e., connections between a SMU network and a non-SMU network shall be protected by a firewall.
- Necessary network and security components shall be implemented, managed, and maintained in a secure manner
- All network and security components shall be configured to provide audit logs for necessary and continual security monitoring.
- Confidentiality and integrity during transmission of critical data shall be ensured using appropriate encryption as required.
- Access to the network components and security devices shall require strict access control and authentication as per the *Access Control Policy*.
- Remote management of critical servers and network components shall only be done through proper encrypted channels.
- All internet connections shall be passed through a content filtering solution to block undesirable web sites
- Appropriate network redundancy shall be built in the environment as per University requirements.
- Network components and the cabling of SMU network shall be protected.
- Detailed network architecture diagram shall be maintained up to date.

- Required documentation in support of all activities, related to network and security components, shall be created and maintained.

Remote Access Policy

- The Technical Team , SMU including (Dy Manager & Associate, IT) shall be responsible for the management and administration of remote access services
- Remote access security shall be controlled and enforced using strong password as per Access Control Policy
- SMU (IT) shall incorporate different methods/types of access to its network from remote hosts, such as, but not limited to P2P Connectivity, MPLS Connectivity, VPN over Internet, SSL VPN Access, VPN Access etc.
- TELNET service shall not be used to access SMU's information system.
- All sensitive data sent through remote access shall be over an encrypted tunnel.
- Any Device that connect to the SMU network must have their personal firewall enabled, operating system patches updated and should have active and updated antivirus software installed.
- For Non-SMU users, access to production systems shall not be permitted unless accompanied by written approvals from the Head IT or respective HOI.
- Components providing remote services must be configured to time out and terminate inactive connections
- The IT Technical team, SMU must ensure that remote access rights to SMU network are provided with the function owners' approved authorization list, and any discrepancies identified are communicated to the respective functions for further appropriate action.

Wireless Guidelines

- Necessary controls shall be established to protect the confidentiality, integrity, availability Band authenticity of data passing over wireless networks
- The wireless infrastructure of SMU shall be logically separate from the wired LAN and further secured with adequate levels of strong user authentication, encryption levels, detection of rogue access points and appropriate physical security controls
- All wireless Access Points/Base Stations connected to the SMU network must be registered, and approved by IT Technical Team, SMU or Head – IT.
- These Access Points/Base Stations shall be subject to periodic penetration tests and audits
- Necessary assessment shall be performed to assess and treat risks involved with wireless communication on a periodic basis.

- Wireless network shall be segregated from other networks based on necessary risk assessment.
- Firewalls shall deny all inbound and outbound traffic that do not support SMU's Interest & University's objectives.
- Current Firewall Access rule set shall be maintained by IT Technical Team under supervision of Dy Manager IT.
- Firewall configuration shall be audited and verified annually by Security Expert of OEM / IT Security Auditors.
- Strict physical access controls shall be in place to secure the firewall.
- Necessary failover or redundancy mechanism as applicable shall be in place
- Firewall logs shall be stored and maintained as per the retention period defined by SMU or based on university requirements
- Firewall logs shall be analysed on a regular basis and any discrepancies shall be logged and acted upon.
- Firewall configuration shall be backed up as per the backup frequency in *Operations Security Policy*
- Changes to firewall configuration shall be streamlined and authorized
- Firewall Management responsibilities shall be listed and assigned.

Network Security Policy

- Network security controls shall be documented and implemented at SMU for logical segregation of SMU networks and for the protection of critical networks, information systems, and applications from unauthorized access, modifications, or destruction by internal or external users.
- The wireless infrastructure of SMU shall be logically separated from the wired LAN and further secured with adequate levels of strong user authentication , encryption levels, detection of rogue access points and appropriate physical security controls.
- The firewall shall be configured and managed to permit access to SMU data from authorized users only and for authorized network services only.
- Intrusion prevention systems (IDS) shall be deployed as appropriate to detect/prevent any intrusions and any unauthorized or malicious activities.
- Network Architecture documentation shall be maintained and access to it shall be restricted on a need-to-know basis.

Instant and Social Messaging

- SMU reserves and intends to exercise the right to review, audit, intercept, access and disclose all messages created, received or sent over the IM system(s) for any purpose.
- The contents of IM messages may be disclosed within SMU to and among authorized personnel without permission of the affected IM user, if reasonable suspicion exists of activities that may violate this or any other SeMU policy
- Social Media platforms and/ or Messaging platforms such as but not limited to Facebook, Twitter, WhatsApp etc. shall not be used by employees and third- parties for any official/professional communication unless approved by designated authority.
- SMU shall consider proactively scanning, blocking or flagging any transmissions, via the SMU network, that contain phrases of profanity or violence, confidential information, or other sensitive data that may expose the organization to operational, legal, reputational, or physical risks.

7. Enforcement

This policy will be reviewed and revised from time-to-time based on business and (or) technological requirements and the same shall be published as revised versions. Any deviation from the above policy should be documented, approved and signed by Head IT.

Related Policies

- Access Control Policy
- Cryptography Policy
- Information Security Incident Management Policy
- Operations Security Policy

-----End of Document-----


Compliance Policy

SMU-ISMS Version - 1.1

(SMU, SMIMS, CRH, SMCPT, SMCON, SMIT)

Revision History

S. No.	Ver. No.	Release Date	Prepared by	Reviewed by	Approved by	Reasons for New Release
1	V1.0	01-08-2019	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) MD Venkatesh Vice Chancellor, SMU	ISMS Implementation
2	V1.1	01-07-2022	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) Rajan S Grewal Vice Chancellor, SMU	Periodic Review


 Head IT (SMU)
 Prepared by
SIKKIM MANIPAL UNIVERSITY
 5th Mile, Tadong
 Gangtok, Sikkim
 Sikkim Manipal University
 737102


 Registrar (SMU)
 Reviewed by
REGISTRAR
SIKKIM MANIPAL UNIVERSITY
 5TH MILE TADONG
 SIKKIM 737102



 Vice Chancellor (SMU)
 Approved by
Dr. (Lt General) Rajan S. Grewal, AVS
Vice Chancellor (SMU)
Sikkim Manipal University
Tadong, Gangtok (Sikkim)

Table of Contents

1. Introduction	4
2. Abbreviations	4
3. Purpose	4
4. Scope	5
5. Roles & Responsibilities	5
6. Policy Description	5
7. Enforcement.....	7

1. Introduction

This policy provides guidance on complying with legal, regulatory and contractual requirements affecting information assets and resources.

The key objectives will be to establish and implement security controls to maintain the following attributes of information:

- Confidentiality i.e. denying unauthorized access to information
- Authenticity i.e. validating the source of message, to ensure that sender is properly identified and
- Integrity i.e. providing the assurance that the message is not modified, accidentally or intentionally.

2. Abbreviations

Abbreviations	Description
SMU	SMU, SMIMS, CRH, SMCPT, SMCON, SMIT
IP	Intellectual Property
ISMS	Information Security Management System
PII	Personally, Identifiable Information
SOP	Standard Operating Procedures

3. Purpose

The purpose of the compliance policy is to avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements of SMU. This includes ensuring that information security is implemented and operated in accordance with the organizational policies and processes of SMU.

4. Scope

- This policy is applicable to all information assets of SMU. An information asset is a definable piece of information stored, transmitted and/ or processed in any manner, which is recognised as value to the University. The types of information assets could be software, physical, paper, service, people and information that is physically or electronically stored and/ or transmitted by any of the aforesaid types of assets.
- All employees on roll and third parties of SMU must adhere to this policy in conjunction with all other policies of SMU.

5. Roles & Responsibilities

The owner of this policy is the Head IT. He shall be responsible for the maintenance and updating of this policy document.

Role	Responsibilities
Head IT	Creation and update of this policy as per requirement
Registrar (SMU)	Review and Approval of this document

6. Policy Description

Compliance with Legal and Regulatory Requirements

SMU will ensure compliance with local and international applicable laws and regulations related to Information Security requirements mentioned in SMU ISMS policies.

Intellectual Property Rights

- Intellectual Property of SMU shall be classified as 'Highly Restricted' asset and provided for use on a 'need-to-know' basis, thus protecting the same against breaches of legal, regulatory and contractual obligations.
- Compliance with legislative, regulatory and contractual requirements related to intellectual property rights will be ensured through the implementation of appropriate procedures.

- Intellectual Property of SMU may include, but not limited to Learning Content, Presentations, Work Products/results of services, Designs, Models, Prototypes, Architecture Diagrams, Computer Programs (including source codes of software and documentation), techniques, Policies & Processes, SOPs & Guidelines, Case Studies, White Papers, Knowledgebase, Specifications that are conceived, created, developed directly or indirectly, whether made solely by SMU or contractors or jointly with others in connection with any work performed for SMU or on behalf of SMU.
- Head IT will support in creating required awareness on prohibited use or re-use of SMU Intellectual Property
- Approval should be obtained from competent authority, HOI or Registrar (SMU) in case SMU Intellectual Property is needed to be shared with any Third Party
- Any breach or non-compliance related to SMU Intellectual Property should be reported to Compliance Officer / Registrar (SMU).

Data Privacy and Protection of records

- Sensitive and confidential information including Personally Identifiable Information (PII) shall be protected by SMU against any loss, destruction, falsification, unauthorized access and release in accordance with legislator, regulatory, contractual and University requirements.
- Personal data must be handled as per *Information Asset Management Policy*. Personal data must only be held for the minimum amount of time and for Compliance or University reasons
- The asset owner must ensure that processes for responding to a breach or potential breach of SMU regulatory requirements are established, maintained, and executed.

Independent Review of Information Security

In order to ensure Information Security is implemented and operated in accordance with the organizational policies and processes, there will be independent reviews of SMU's approach to managing information security and its implementation held at planned intervals or when significant changes occur.

Independent review of Information Security should be conducted through either Internal or External Audits. For more information, refer the *Information Security Management System Audit* process.

For technical testing of Information Systems, the prior approval of the IT functions/Asset Owner should be obtained. Adequate precautions should be taken before the execution of technical testing. The testing tools should be under the custody of the SMU (IT) and should be physically and logically protected.

Other than independent review of Information Security through Internal and External Audits, Function HOD in their respective functional areas should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies and other security requirements.

7. Enforcement

This policy will be reviewed and revised from time-to-time based on business and (or) technological requirements and the same shall be published as revised versions. Any deviation from the above policy should be documented, approved and signed by Head IT.

Related Policies

- Information Asset Management Policy
- Information Security Incident Management Policy
- Organization of Information Security Policy
- Information Security Management System Audit Process

-----End of Document-----

Human Resource Security Policy


SMU-ISMS
Version -1.1

(SMU, SMIMS, CRH, SMCPT, SMCON, SMIT)



Revision History

S. No.	Ver. No.	Release Date	Prepared by	Reviewed by	Approved by	Reasons for New Release
1	V1.0	01-08-2019	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) MD Venkatesh Vice Chancellor, SMU	ISMS Implementation
2	V1.1	01-07-2022	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) Rajan S Grewal Vice Chancellor, SMU	Periodic Review


Head IT (SMU)
Prepared by
SIKKIM MANIPAL UNIVERSITY
5th Mile, Tadong
Gangtok, Sikkim
Sikkim Manipal University
737102


Registrar (SMU)
Reviewed by
REGISTRAR
SIKKIM MANIPAL UNIVERSITY
5TH MILE TADONG
SIKKIM 737102



Vice Chancellor (SMU)
Approved by
Dr. (Lt. Gen.) Rajan S. Grewal, AVS
Vice Chancellor (SMU)
Sikkim Manipal University
Tadong, Gangtok (Sikkim)



Table of Contents

1. Introduction	4
2. Abbreviations	4
3. Purpose	4
4. Scope	5
6. Policy Description.....	5
7. Enforcement	7

1. Introduction

This policy defines the security requirements that need to be integrated with the Human Resources (HR) processes including screening of candidates, recruitment process, during employment and upon change of role, exit or termination at SMU.

2. Abbreviations

Abbreviations	Description
SMU	SMU, SMIMS, CRH, SMCPT, SMCON, SMIT, SMUDDE
HR	Human Resources
ISMS	Information Security Management System
JD	Job Description
NDA	Non-Disclosure Agreement

3. Purpose

The purpose of this policy is to ensure that:

- Screening process is conducted satisfactorily so that the right candidates are recruited, leading to better protection of SMU information assets.
- Employees are bound by contract and non-disclosure agreements about information assets of SMU.
- Employees understand their responsibilities and roles regarding information security
- Risk due to human error, theft, fraud or misuse of information assets and facilities is reduced.
- A formal disciplinary process to act against employees who have committed a security breach or who have violated IT security policies is implemented.
- Information assets are recovered by SMU upon change of role, exit or termination of employees.

4. Scope

- This policy is applicable to all information assets of SMU. An information asset is a definable piece of information stored, transmitted and/ or processed in any manner, which is recognised as value to the University. The types of information assets could be software, physical, paper, service, people and information that is physically or electronically stored and/ or transmitted by any of the aforesaid types of assets.
- All employees and third parties of SMU must adhere to this policy in conjunction with all other policies of SMU.

5. Roles & Responsibilities

The owner of this policy is jointly Head IT & HR Head for compliance . The IT Head shall be responsible for the maintenance and updating of this policy document.

Role	Responsibilities
IT Head	Creation and update of this policy as per requirement
Registrar (SMU)	Review and Approval of this document

6. Policy Description

Information security controls shall be designed and integrated with the HR processes to ensure that employees of the SMU role and third party understand their responsibilities and are suitable for the roles they are considered so as to reduce the risk of theft, fraud, or misuse of information assets.

Prior to Employment

- For any position at SMU, Job Description (JD) should be documented with information security roles and responsibilities.
- All candidates for positions within SMU shall be subjected to a formal interviewing and selection process that is used by HOD to make informed hiring decisions. This on-boarding process should be aligned to the Information Security policy where appropriate and applicable, including candidate background screening as directed by SMU.
- For any third-party, information security roles and responsibilities shall be defined and documented as a part of the service contract document.

- Temporary staff and contractor as a part of the onboarding process shall sign an NDA ('Non-Disclosure Agreement') together with the service contract
- After successful recruitment, employees shall sign an NDA ('Non-Disclosure Agreement') together with the employment contract, Code of Conduct document
- The HR shall follow the candidate on-boarding process for inducting a new employee and change of role, transfer/separation of employees from SMU.

During Employment

- The Head IT shall ensure that importance of Information security is communicated to all employees to maintain an information conscious culture at SMU
- The Head IT in conjunction with the HR team shall ensure that employees are periodically made aware of their security responsibilities by taking appropriate actions such as awareness drives, education, and training or similar programs
- The HR shall maintain records and track completion progress of all awareness drives and employee awareness trainings.
- HR shall define formal disciplinary process and ensure that employees are made aware of this process which may be initiated against them if they violate or commit any kind of security breach.
- The employees must also be made aware of the *Information Security Incident Management Process* to ensure information security incidents are reported to the Head IT on a timely basis, thereby minimizing the impact of the incidents.

Termination or Change of Employment

- HR shall ensure that change or transfer of employment responsibilities of the employee shall be clearly defined, assigned and communicated to the employee upon change or transfer of responsibilities
- In the event of a change in responsibility of an employee or third parties, IT department is required to ensure that the relevant access rights are revoked or modified as required
- HR shall ensure that exit or termination of employment responsibilities shall be clearly defined, assigned and communicated to the employees of the HR team who would perform the duties
- HR should initiate the termination process on the employee's last working day
- HR shall formalize a termination process. This process shall include the return of all issued assets such as software, corporate documents, equipment, access cards, manuals and/or any other assets that are the property of SMU.

- HR, Facilities and IT shall be required to ensure that the access rights of all employees and third parties to information assets and information processing facilities, shall be revoked upon termination of their employment, contract or agreement
- Access rights of employees should be disabled by the close of University hours of the last working day
- Temporary staff, contractors, and vendors' access should be disabled on the last working day identified by their reporting manager.

7. Enforcement

This policy will be reviewed and revised from time-to-time based on business and (or) technological requirements and the same shall be published as revised versions. Any deviation from the above policy should be documented, approved and signed by Head IT.

Related Policies

- Information Security Incident Management Policy
- Organization of Information Security Policy
- Physical and Environmental Security Policy

-----End of Document-----


Secure Information Systems Development and Maintenance Policy

SMU-ISMS Version - 1.1

(SMU, SMIMS, CRH, SMCPT, SMCON, SMIT)

Revision History

S. No.	Ver. No.	Release Date	Prepared by	Reviewed by	Approved by	Reasons for New Release
1	V1.0	01-08-2019	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) MD Venkatesh Vice Chancellor, SMU	ISMS Implementation
2	V1.1	01-07-2022	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) Rajan S Grewal Vice Chancellor, SMU	Periodic Review


 Head IT (SMU)
 Prepared by
SIKKIM MANIPAL UNIVERSITY
 5th Mile, Tadong
 Gangtok, Sikkim
 Sikkim Manipal University
 737102


 Registrar (SMU)
 Reviewed by
REGISTRAR
SIKKIM MANIPAL UNIVERSITY
 5TH MILE TADONG
 SIKKIM 737102



 Vice Chancellor (SMU)
 Approved by
Dr. (Lt. General) Rajan S. Grewal, AVS
Vice Chancellor (SMU)
Sikkim Manipal University
 Tadong, Gangtok (Sikkim)

Table of Contents

1. Introduction	4
2. Abbreviations	4
3. Purpose	4
4. Scope	4
5. Roles & Responsibilities	5
6. Policy Description	5
7. Enforcement.....	8

1. Introduction

For information systems to be robust and capable of safeguarding against threats, they must be designed and maintained with appropriate controls from inception. This policy defines the controls to be implemented throughout the lifecycle of information systems including development and maintenance.

2. Abbreviations

Abbreviations	Description
SMU	SMU, SMIMS, CRH, SMCPT, SMCON, SMIT
ISMS	Information Security Management System

3. Purpose

The purpose of this policy is to ensure that information security is an integral part across the entire lifecycle of all information systems developed or maintained at SMU. This also includes information systems which provide services over public networks.

4. Scope

- This policy is applicable to all information assets of SMU, SMCPT, SMCON, SMIT, SMUDDE, HSS. An information asset is a definable piece of information stored, transmitted and/ or processed in any manner, which is recognised as value to the University. The types of information assets could be software, physical, paper, service, people and information that is physically or electronically stored and/ or transmitted by any of the aforesaid types of assets.
- All employees and third parties of SMU Institutions must adhere to this policy in conjunction with all other policies of SMU.

5. Roles & Responsibilities

The owner of this policy is the Head – IT, He shall be responsible for the maintenance and updating of this policy document.

Role	Responsibilities
Head – IT	Creation and update of this policy as per requirement
Registrar (SMU)	Review of this document

6. Policy Description

Application Security Training

- All members of the software development team shall receive appropriate training to stay informed about security basics. Individuals in technical and management roles (developers, testers, Project Managers) who are directly involved with the development of software programs shall attend at least one security training each year.
- Basic software security training shall cover foundational concepts like:
 - Fundamentals of Application Security
 - Secure design guidelines
 - Threat modelling
 - Secure coding including programming guidelines
 - Security Testing
 - Privacy design, development and testing best practices

Secure Development Requirements

- All projects shall be developed in a secured environment. Project security requirements shall be captured in collaboration with stakeholders and the Application/Product Owner. Security design requirements must be documented and maintained.

- All projects source code shall be accessed by using version control process. Source code access shall be limited to specific individuals and access shall be granted on a 'need basis'
- Source codes with version control shall be backed up regularly to a secure location
- If any defects or bugs are identified, they shall be fixed by the developer
- Logical separation between different environments (Development, Testing) shall be maintained for projects
- Changes to systems within the development life cycle shall be controlled by the use of formal change control procedures:
 - Request for Change by the customer shall be captured and documented
 - Project Manager shall perform an impact analysis and evaluate the risks arising from the impact of the change
 - He/she shall analyze scope, cost, schedule, quality associated with the change and then approve the change
 - Once the change is implemented, the effect of the change shall be monitored and
 - A roll back plan shall be developed to restore the system to its original state in the event the implementation of the change has unforeseen effects
- Code review shall be initiated and continued throughout the development cycle till the final product is delivered. Testing of security functionality shall be carried out during development and
- University critical application/product developed shall undergo Vulnerability Assessment either by internal resource or a third party or the customer. Based on the vulnerabilities identified and the severity levels, remediation action shall be implemented to address the vulnerabilities. Refer *Operations Security Policy*.

Outsourced Development

SMU (Head IT) shall supervise and monitor the activities of system development that is outsourced to any third party.

Secure System User Acceptance Testing Requirements

- Test data should be backed up at different stages of testing. Acceptance test should be carried out using test data, which should be similar to operational data
- Any operational data that is classified as confidential should be masked prior to using it in the test environment. Appropriate authorization should be taken each time prior to copying any operational data in the test environment
- Logs of copying and activities on production data in the test environment should be recorded to maintain audit trail.

- Prior to deploying any change to the production environment, test for user acceptance should be performed in the test environment.

Security guidelines for Production environment

- There should be separate system hardware for development, test and production environments, wherever applicable. There should be a strategy for day-to-day disk space management on the production environment
- Daily backup should be taken for the data, logs and configurations in the production environment
- Physical access to the production environment shall be monitored. A strong password policy shall be enforced in the production environment. Access to the production environment should only be given after appropriate approvals
- Test data should be backed up and purged prior to deploying into production environment
- Application logs should be maintained for at least six months for all University–critical applications and
- Application owner should ensure that auditing should be done on a periodic basis for all Application logs to detect any unauthorized activity.

Security guidelines for Maintenance of Applications

This involves provision of end to end application maintenance and support services for tailor-made applications as well as for platform-based solutions.

- Application support and maintenance services include enhancements, Security patching, Windows patching and DB patching need to be done Regular intervals.
- Change Request Management process should follow during any change in the environment
- 24X7 support when Required for mission critical projects, L1, L2 and L3 support, production support, service help desk, monitoring, etc.

7. Enforcement

This policy will be reviewed and revised from time-to-time based on business and (or) technological requirements and the same shall be published as revised versions. Any deviation from the above policy should be documented, approved and signed by Head IT.

Related Policies

- Information Security Incident Management Policy
- Operations Security Policy
- Organization of Information Security Policy

-----End of Document-----



Service Vendor Management Policy


SMU-ISMS Version - 1.1

(SMU, SMIMS, CRH, SMCPT, SMCON, SMIT)



Revision History

S. No.	Ver. No.	Release Date	Prepared by	Reviewed by	Approved by	Reasons for New Release
1	V1.0	01-08-2019	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) MD Venkatesh Vice Chancellor, SMU	ISMS Implementation
2	V1.1	01-07-2022	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) Rajan S Grewal Vice Chancellor, SMU	Periodic Review


Head IT (SMU)
Prepared by
SIKKIM MANIPAL UNIVERSITY
5th Mile, Tadong
Gangtok, Sikkim
Sikkim Manipal University
737102


Registrar (SMU)
Reviewed by
REGISTRAR
SIKKIM MANIPAL UNIVERSITY
5TH MILE TADONG
SIKKIM 737102



Vice Chancellor (SMU)
Approved by
Dr. (Lt. General) Rajan S. Grewal, AVS
SIKKIM MANIPAL UNIVERSITY
Tadong, Gangtok (Sikkim)



Table of Contents

1. Introduction	4
2. Abbreviations	4
3. Purpose	4
4. Scope	4
5. Roles & Responsibilities	5
6. Policy Description.....	5
7. Enforcement.....	9



1. Introduction

The Service Vendor Management Policy is designed to ensure protection of the hardware and software assets of Sikkim Manipal University and its Colleges (herein referred to as 'SMU') that is accessible by vendors/suppliers. This includes maintaining an agreed level of service delivery with vendor/suppliers.

2. Abbreviations

Abbreviations	Description
CRM	Customer Relationship Management
ISMS	Information Security Management System
SMU	SMU, SMIMS, CRH, SMCPT, SMCON, SMIT, SMUDE
SLA	Service Level Agreement
TAT	Turn Around Time

3. Purpose

The purpose of this policy is to ensure appropriate security controls for protection of the University's assets that are accessible to third-party vendors.

4. Scope

All employees and third parties of SMU & it's colleges must adhere to this policy in conjunction with all other policies of SMU. Anyone having any query regarding this policy shall consult with the Head IT or Registrar (SMU).



5. Roles & Responsibilities

The owners of this policy is the Head IT and designated assignee shall be responsible for the maintenance and updating of this policy document.

Role	Responsibilities
Head – IT	Creation and update of this policy as per requirement
Registrar (SMU)	Review and Approval of this document

6. Policy Description

SMU & its Colleges shall implement appropriate security controls to protect its assets that are accessible to third-party vendors.

Here are some specific terms and their definitions:

Term	Definition
Vendor	Vendor is the organization or individual providing services to SMU. The Vendors may provide services related to 'Delivery Services' or 'Product Supply' or 'Support Services'. Vendors may include: <ul style="list-style-type: none">• Partners for Services and Products.• Consultants for Services• Contractors for Services• Free Lancers for Services• Vendors for Support Services
Services	University specific work to support delivery. E.g.: Development of online training content.
Product Supply	Services related to the supply of critical IT Infrastructure equipment & devices that support key University operations & their maintenance. E.g.: Supply of network devices like routers, switches, firewalls. E.g.: Supply of servers & computing devices.
Support Services	Non-University specific work / 'non-core' services being provided to SMU. Services like 'material movement' of technology assets / equipment to and from SMU facility by vendors etc.
Outsourcing	Subcontracting of the 'University specific work' or 'core work' to a non-SUM entity. E.g.: Outsourcing of application development related work to a vendor for a fixed period of time.



Vendor Relationship Manager	Vendor Relationship Manager is required to monitor the performance with respect to the service levels specified in the service agreement of the Vendor.
Vendor SLA	Service Level Agreements shall establish SMU's expectations with regard to Vendor performance and quality in a number of ways. Failure to meet SLA targets shall attract penalties. SLA metrics may include, but not limited to: <ul style="list-style-type: none">• Availability and Uptime• Response time & Resolution time• First Time Resolution• Turn Around Time (TAT) / Cycle time• Accuracy % or Defect rate• Notification in advance of network changes that may affect users.

- Depending on the nature of work, Vendors' services to SMU also include, but not limited to:
 - Development of applications and / or systems.
 - SaaS Software as a Service from vendors
 - PaaS Platform as a Services from vendors
 - IaaS Infrastructure as a Service from vendors
 - Hosting Services (e.g. cloud computing, applications, archiving facilities)
 - Managed services for Vendor may include, but are not limited to:
 - Remote infrastructure management and monitoring
 - Applications support
 - End User support
 - Email, messaging and fax Vendors
 - Consulting Vendors including strategic and advisory services

Vendor Details

The following information must be maintained for each vendor that the University function uses:

- The name of the vendor
- Locations and Name of University function supported by the vendor
- Locations from where the services will be delivered by the vendor
- The name and contact information of the key University contact at the vendor
- The name and contact information of the SMU Vendor Relationship Manager
- A description of each service outsourced to the vendor
- The service level agreements (SLA) with the vendor (if applicable)
- The start and end date of the service agreements between SMU and the vendor.



- Terms & References in the agreement must be clearly defined.
- Roles & Responsibility in PO, Agreement and MOM must be defined with clarity.

Due Diligence and Risk Assessment

Control Environment Reviews shall be conducted prior to entering into a service agreement with a vendor and while the service agreement is in effect.

The control environment review must include:

- The controls identified in the Risk Assessment process
- Each of the locations from where services are provided to SMU.

The following SMU functions or teams must be consulted before beginning service agreements negotiations:

- Hon'ble Vice Chancellor
 - Head of Institutions (HOI)
 - Head of Unit (HOU)
 - Registrar (SMU)
 - Chairmen IPC / UPC Committee.
 - CFA (Competent Financial Authority)
 - Senior Finance Officer
-
- Vendor risk must be assessed every time there is a change in the scope of service.
 - A Vendor Relationship Manager should monitor the performance with respect to the service levels specified in the service agreement.
 - Head of IT may rely on SMU resource, third party assessments or an external consulting firm to conduct a Control Environment Review.
 - If any other SMU & its colleges has prior relationship with the vendor and has conducted an adequately scoped review of the vendor, additional reviews of the control environment may not be required. However, on-going review frequency must be met.

Review Frequency

Based on the Risk Assessment conducted on the vendor:

- A risk level must be assigned to the vendor.
- The risk level assigned to the vendor must determine the frequency of review and must follow the schedule stated below:



Vendor Risk Level	Review Requirements	Review Frequency		
Low	Appropriately scoped control environment review must be conducted	At the discretion of the Function/Information Security Team		
Medium	Appropriately scoped control environment review must be conducted	At the discretion of the Function/Information Security Team		
High	<ul style="list-style-type: none">• Vendor must implement Corrective action for risks identified and compensating controls around them• Review shall be conducted on the implementation of compensating controls by the vendor periodically	<table border="1"><tr><td>Continuous review</td></tr><tr><td>Monthly review</td></tr></table>	Continuous review	Monthly review
Continuous review				
Monthly review				

Service Agreement

A service agreement with the vendor shall be in place before the vendor begins the service.

- The service agreement shall address audit reporting and shall contain provision for SMU to obtain a copy of the report. (If available, internal audit reports of the vendor related to the services need to be provided to SMU)
- The service agreement must include provisions requiring the vendor to notify SMU of any security-related incidents affecting the confidentiality, integrity and availability of SMU information
- All service agreements must have an exit plan, including, but not limited to renegotiation/ termination of contract
- The agreement must include the following, but not limited to:
 - Controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during the agreement
 - Restrictions on copying
 - Agreement must include the right to audit, including, but not limited to the right to assess performance on a monthly basis against critical controls identified during the risk assessment
 - Agreement must include non-disclosure, data privacy and confidentiality clauses



7. Enforcement

This policy will be reviewed and revised from time-to-time based on business and (or) technological requirements and the same shall be published as revised versions. Any deviation from the above policy should be documented, approved and signed by Head IT.

Related Policies

- Access Control Policy
- Information Security Incident Management.

-----End of Document-----



Physical Environment Security Policy


SMU-ISMS Version - 1.1

(SMU, SMIMS, CRH, SMCPT, SMCON, SMIT)



Revision History

S. No.	Ver. No.	Release Date	Prepared by	Reviewed by	Approved by	Reasons for New Release
1	V1.0	01-08-2019	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) MD Venkatesh Vice Chancellor, SMU	ISMS Implementation
2	V1.1	01-07-2022	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) Rajan S Grewal Vice Chancellor, SMU	Periodic Review


Head IT (SMU)
Prepared by
SIKKIM MANIPAL UNIVERSITY
5th Mile, Tadong
Gangtok, Sikkim
Sikkim Manipal University
737102


Registrar (SMU)
Reviewed by
REGISTRAR
SIKKIM MANIPAL UNIVERSITY
5TH MILE TADONG
SIKKIM 737102



Vice Chancellor (SMU)
Approved by
Dr. (Lt. General) Rajan S. Grewal, AVS
SIKKIM MANIPAL UNIVERSITY
Tadong, Gangtok (Sikkim)

Table of Contents

1. Introduction	4
2. Abbreviations	4
3. Purpose	4
4. Scope	4
5. Roles & Responsibilities	5
6. Policy Description.....	5
7. Enforcement.....	6

1. Introduction

It is important to protect the information assets at the same time, it is equally important to regulate the first level of access to these assets to preventing unauthorized physical access, damage and interference to these assets and ensuring their continued availability is vital.

2. Abbreviations

Abbreviations	Description
SMU	SMU, SMIMS, CRH, SMCPT, SMCON, SMIT
ISMS	Information Security Management System

3. Purpose

The purpose of this policy is to prevent unauthorized physical access, damage, and interference to the information processing assets/physical assets of SMU. This also includes prevention of loss, damage, theft or compromise and interruption to the organization's operations.

4. Scope

- The SMU Information Security Policy is applicable to all information assets of SMU, SMIMS, CRH, SMCPT, SMCON, SMIT, SMUDDE, HSS. An information asset is a definable piece of information stored, transmitted and/ or processed in any manner, which is recognised as value to the University. The types of information assets could be software, physical, paper, service, people and information that is physically or electronically stored and/ or transmitted by any of the aforesaid types of assets.
- All employees and third parties of SMU must adhere to this policy in conjunction with all other policies of SMU. Anyone having any query regarding this policy shall consult with the SMU Information Security core team.

5. Roles & Responsibilities

The owner of this policy is the Head – Facilities, who shall be responsible for the maintenance and updating of this policy document.

Role	Responsibilities
Head – Facilities	Creation and update of this policy as per requirement
Registrar (SMU)	Review & Approval of this document

6. Policy Description

6.1 Physical Security

Physical security perimeters considered for current scope of implementation,

Physical access controls that restrict access and monitor entry to the SMU facilities shall be implemented as follows:

- All the common areas, work areas and restricted areas in SMU Campus of each location /premises shall have an identified custodian who shall authorize access.
- Any outward / inward material movement especially from Stores and all critical sections shall be supervised by the security
- Employees, Service Providers and visitor groups shall be easily distinguishable:
 - Identification badges shall be visibly distinct for different category of entrants (Different color lanyards for different categories of entrants)
 - Employees shall be provided with photo ID badges
- Entry points on the floor shall have a Biometric reader
- Biometric access rights shall be provided to employees. The HR SPOC shall authorize the access.
- Terminated SMU personnel shall have all physical access rights, including access to restricted areas, revoked or removed on the last working day.

Note: For physical access to server rooms and Data Center facilities, refer *Access Control Policy* which is owned by IT.

Environmental Security

- Risk assessment shall be conducted for each facility to identify environmental controls commensurate with the risks;
- The risks scenarios shall include:
 - Natural and man-made disasters
 - Equipment security
 - Center or site security
- The following minimum environmental controls shall be evaluated for implementation:
 - Heat / smoke detectors shall be in strategic locations throughout the facility.
 - Sprinkler systems shall be installed in the basement.
- For areas such as server rooms, additional environmental conditions shall be in place such as:
 - Alarm systems to alert rise in temperature beyond optimum levels
 - Raised floor and false ceiling for routing network and electrical cables.
- All equipment, such as fire detector, DG, UPS etc. shall be inspected as per the AMC schedule.

7. Enforcement

This policy will be reviewed and revised from time-to-time based on business and (or) technological requirements and the same shall be published as revised versions. Any deviation from the above policy should be documented, approved and signed by Head IT.

Related Policies

- Access Control Policy
- Business Continuity Management Policy
- Information Security Incident Management Policy

-----End of Document-----


Business Continuity Management Policy

**SMU-ISMS
Version -1.1**

(SMU, SMIMS, CRH, SMCPT, SMCON, SMIT)

Revision History

S. No.	Ver. No.	Release Date	Prepared by	Reviewed by	Approved by	Reasons for New Release
1	V1.0	01-08-2019	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) MD Venkatesh Vice Chancellor, SMU	ISMS Implementation
2	V1.1	01-07-2022	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) Rajan S Grewal Vice Chancellor, SMU	Periodic Review


 Head IT (SMU)
 Prepared by
SIKKIM MANIPAL UNIVERSITY
 5th Mile, Tadong
 Gangtok, Sikkim
 Sikkim Manipal University
 737102


 Registrar (SMU)
 Reviewed by
REGISTRAR
SIKKIM MANIPAL UNIVERSITY
 5TH MILE TADONG
 SIKKIM 737102


 Vice Chancellor (SMU)
 Approved by
Dr. (Lt General) Rajan S. Grewal, AVS
Vice Chancellor (SMU)
Sikkim Manipal University
 Tadong, Gangtok (Sikkim)

Table of Contents

1. Introduction	4
2. Abbreviations.....	4
3. Purpose	4
4. Scope.....	5
5. Roles & Responsibilities	5
6. Policy Description	5
7. Enforcement	8

1. Introduction

This policy defines the controls to establish a framework to counteract interruptions to business activities and to protect the critical business processes from the effects of business disruptions such as major failures, disasters, etc. and their timely resumption.

The key objective here will be to promote organizational survival by ensuring that critical business processes can continue, or be recovered in a timely manner, following a disruption, thus ensuring:

- Operations are not adversely affected, thus maintaining the quality of management and meeting statutory and regulatory requirements of the business.
- Students /Patients / Internal Employees expectations and quality of services continue to be met, or managed, in such a way that customers / stakeholders are retained, and new business opportunities met.

2. Abbreviations

Abbreviations	Description
BCP	Business Continuity Plan
BIA	Business Impact Analysis
SMU	SMU, SMIMS, CRH, SMCPT, SMCON, SMIT, SMUDDE
DR	Disaster Recovery
ERT	Emergency Response Team
ISMS	Information Security Management System
SPOC	Single Point of Contact

3. Purpose

The purpose of this policy is to ensure the business continuity of University / CRH's all Critical Services even in the event of natural or man-made disasters/ interruptions and to protect its critical business processes from the effects of Operational disruptions.

4. Scope

- This policy is applicable to all information assets of SMU. An information asset is a definable piece of information stored, transmitted and/ or processed in any manner, which is recognised as value to the business. The types of information assets could be software, physical, paper, service, people and information that is physically or electronically stored and/ or transmitted by any of the aforesaid types of assets.
- All employees and third parties of SMU must adhere to this policy in conjunction with all other policies of SMU.

5. Roles & Responsibilities

The owner of this policy is the Head IT, he shall be responsible for the maintenance and updating of this policy document.

Role	Responsibilities
HEAD IT	Creation and update of this policy as per requirement
REGISTRAR (SMU)	Review and Approval of this document

6. Policy Description

Business Continuity Plan

- A BCP Team shall be created to handle crisis/emergency situations
- Employees shall be made aware of SPOCs that they can contact in case of any crisis
- It shall also be ensured that all employees understand BCP and how it relates to their respective service areas.

BCP Team

A BCP Core Team shall be created and it will, at a minimum, comprise of the following:

- HOI, HOU, HOD, HOO
- Head GS & HOD Engineering
- Head IT

- SMU /SMIT (IT) Team & Other team members nominated by the BCP core team.

Business Continuity Planning, done by the BCP Team, will involve the following processes:

- Business Impact Analysis (BIA)
- Risk Assessment
- Risk Management
- Risk Monitoring and Review

Head IT will manage and head the BCP activities.

The Head IT will also be responsible for:

- Developing an enterprise wide BCP and prioritization of business objectives and critical operations that are essential for recovery.
- Business Continuity Planning to include the recovery, resumption, and maintenance of all aspects of the business, not just recovery of the technology components.
- Regularly updating Business Continuity Plans based on changes in business processes, audit recommendations and lessons learned from annual testing.
- Following a cyclical, process-oriented approach that includes a Business Impact Analysis (BIA), risk assessment, management and monitoring, and testing.
- Considering all factors and deciding upon declaration of a “crisis” and restoration of normal business operations.

Business Impact Analysis

- A Business Impact Analysis (BIA) will be undertaken on a yearly basis or as decided by management to identify critical business processes
- Risk Assessments will be performed periodically to identify potential threats which can lead to disruptions and minimize the impact of the risks to an acceptable level, for all the identified critical services
- All Function Heads will be required to perform a BIA for each key business system that is used in his/her area of responsibility
- The assessment will identify and define the criticality of key business systems and the repositories that contain the relevant and necessary data for those business systems
- The assessment will also define and document the BC & DR Plan for the identified business system.

Business Continuity Plans

- Each key business system will be part of the BCP for critical situations like hardware, software or networks becoming critically difunctional (short- or long-term outages), critical system failures, unavailability of the work facility or employees due to unforeseen circumstances etc.
- This plan should include an explanation of the magnitude of information or system unavailability in the event of an outage and the process that would be implemented to continue operations during the outage. In addition, the feasibility of utilizing alternative off-site computer operations should be addressed.

Specifically, the BCP should include:

- A plan for continuing operations in the event of temporary hardware, software or Network outage. This plan should contain information relating to the end user process for continuing operations
- A DR Plan for returning functions and services to normal on-site operations when a disaster is over and
- A procedure for periodic testing, review and revision of the BCP for all affected Systems, as a group or individually as needed.

Disaster Recovery Plan

- It will be ensured that a Disaster Recovery plan is in place for all critical IT systems
- Disaster Recovery sites will be identified such that the DR site is at a minimum of 10 kms away from the primary site with necessary infrastructure to support recovery needs
- Depending on the severity and impact of an adversity, disaster recovery plans will be formulated
- A disaster recovery plan as a part of the BCP will dictate every aspect of the recovery process which will include the following:
 - The events that denote possible disasters
 - Authority given to the HOI to declare a disaster and thereby put the plan into effect
 - The sequence of events necessary to prepare the backup site once a disaster has been declared
 - The roles and responsibilities of all key personnel with respect to carrying out the plan
 - An inventory of the necessary hardware and software required to restore operations

- A schedule, listing the personnel that will be staffing the backup site, including a rotation schedule to support ongoing operations without burning out the team members.
- An emergency response team (ERT) will be created to carry out all activities as listed in the DR plan
- The DR plan will be annually updated to reflect the latest changes in the SMU systems.
- Mock disaster drills will be conducted semi-annually to test the effectiveness of the DR plan.

7. Enforcement

This policy will be reviewed and revised from time-to-time based on business and (or) technological requirements and the same shall be published as revised versions. Any deviation from the above policy should be documented, approved and signed by Head IT.

Related Policies

- Access Control Policy
- Information Asset Management Policy
- Communication Security Policy
- Human Resource Security Policy
- Information Security Incident Management Policy
- Operations Security Policy
- Organisation of Information Security Policy
- Physical and Environmental Security Policy

-----End of Document-----


Cryptography Policy

**SMU-ISMS
Version -1.1**


(SMU, SMIMS, CRH, SMCPT, SMCON, SMIT)

Revision History

S. No.	Ver. No.	Release Date	Prepared by	Reviewed by	Approved by	Reasons for New Release
1	V1.0	01-08-2019	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) MD Venkatesh Vice Chancellor, SMU	ISMS Implementation
2	V1.1	01-07-2022	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) Rajan S Grewal Vice Chancellor, SMU	Periodic Review


 Head IT (SMU)
 Prepared by
SIKKIM MANIPAL UNIVERSITY
 5th Mile, Tadong
 Gangtok, Sikkim
 Sikkim Manipal University
 737102


 Registrar (SMU)
 Reviewed by
REGISTRAR
SIKKIM MANIPAL UNIVERSITY
 5TH MILE TADONG
 SIKKIM 737102


 Vice Chancellor (SMU)
 Approved by
Dr. (Lt General) Rajan S. Grewal, AVS
Vice Chancellor (SMU)
Sikkim Manipal University
 Tadong, Gangtok (Sikkim)

1. Table of Contents

1. Introduction	Error! Bookmark not defined.
2. Abbreviations	Error! Bookmark not defined.
3. Purpose	4
4. Scope	4
5. Roles & Responsibilities	Error! Bookmark not defined.
6. Policy Description	5
7. Related Policies	8

1. Introduction

This policy document defines the controls that need to be implemented to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information stored, transmitted and hosted by all IT systems and equipment that is owned, leased or rented by Manipal Global Education Services Pvt. Ltd. (herein referred to as 'MaGE').

2. Abbreviations

Abbreviations	Description
HEAD IT	Head IT
CIO	Chief Information Officer
ISMS	Information Security Management System

3. Purpose

The purpose of this policy is to define the controls to:

- Define and implement encryption on data in storage and/or in motion and
- Manage encryption keys throughout their lifecycle – from creation to destruction.

4. Scope

- This policy is applicable to all information assets of SMU. An information asset is a definable piece of information stored, transmitted and/ or processed in any manner, which is recognized as value to the business. The types of information assets could be software, physical, paper, service, people and information that is physically or electronically stored and/ or transmitted by any of the aforesaid types of assets.
- All employees and third parties of SMU must adhere to this policy in conjunction with all other policies of SMU.

5. Roles & Responsibilities

The owner of this policy is the Head –IT. He will be responsible for the maintenance and updating of this policy document.

Role	Responsibilities
HEAD IT	Creation and update of this policy as per requirement
Registrar, SMU	Review and Approval of this document

6. Policy Description

MaGE shall ensure confidentiality of information, which is either stored, processed or transmitted using information assets.

Use of Cryptographic Controls

- Cryptographic requirements shall be assessed for possible implementation when the requirements exist to enforce confidentiality, data integrity, non-repudiation, authentication and data origin
- The use and selection of cryptographic requirements should be based on criticality and risk assessments and meet cost-benefit and performance tests
- The recovery procedure for the data must be documented
- A log of keys should be kept for each user. Minimum and maximum retention period should be agreed with the information owner
- Cryptographic services shall not interfere with any legal or regulatory or any other compliance requirements (e.g. data privacy, financial regulations, records retention, content inspection, anti-malware requirements, IDS/IPS, data leakage prevention, surveillance, e- discovery, forensics, etc.)
- The Head – Data Center & Cloud Services/CIO shall approve all cryptographic products, processes, and standards before using /implementing in the environment
- Generally, only cryptographic mechanisms that are regarded as strong must be used. Legacy encryption algorithms like 3DES or earlier, symmetric keys less than 256 bits, asymmetric keys less than 1024 and hash algorithms other than SHA-2 must not be used unless a waiver has been approved by the Head – Data Center & Cloud Services/CIO. For the use of specific cryptographic mechanisms refer to internationally accepted standards.

Cryptographic Control for Data in Storage

- Encryption of data on hard disks of portable devices wherever it is possible (e.g. laptop, tablet):
 - IT Delivery & Operations shall incorporate full disk encryption for all mobile devices like Laptops which may potentially have an opportunity for storing sensitive data and access must be protected by a password
 - IT Delivery & Operations shall ensure that the allocated laptop to the users are encrypted
 - Users shall change password in the first login instances to prevent users using default passwords. Refer to *Access Control Policy*
 -
- Storage of data on Cloud:
 - All “Highly Restricted”, and/or “Confidential” information stored within the cloud environment should be encrypted and access to the information be provided on a “need-to-know” basis

Cryptographic Controls for Data in Transit

- If “Highly Restricted”, and/ or “Confidential” information is transmitted outside of SMU or over public networks, then the use of encryption is mandatory.
- For traffic over internal company networks and trusted internal third-party networks criticality and risks shall be considered when deciding if encryption should be used
- Network traffic between SMUI and third-party shall be encrypted.
- Application traffic should be encrypted
- Administrative traffic on the LAN shall be encrypted
- In a Client/Server environment, identifiers and passwords shall be encrypted between the client and the server; data must also be encrypted between the client and the server
- IT should implement Transport Layer Security (TLS) for all emails with sensitive data
- If wireless access to network is implemented, wireless shall meet authorization & strong authentication (e.g. WPA2) and encryption protocols consistent with industry leading practices.

Key Management

- The keys must be created on a secure and appropriate system
- Personal keys must be created in a way that only the person using the key has access to the key
- If system keys need to be distributed, confidentiality must be ensured. The responsible administrators must either manually distribute the keys or ensure during and after transmission that the key is installed only on the intended system
- Personal keys must be protected through a strong password (chosen by the end-user) and must be only accessible for the respective end-user
- Access control for system keys must be configured as restrictive as possible. Only system administrators and the respective applications must have access. Unauthorized access must not be possible and
- Keys are generated afresh in case of suspected compromise
- Internal systems are installed and managed securely with appropriate physical and logical controls
- Secure backup of internal private keys is maintained on an independent secure media which provides a source for key recovery
- The backed-up keys are protected from physical and environmental threats.
- Cryptographic keys are destroyed in a secure manner when they are no longer required
- Adequate provision is made for different cryptographic keys for different uses and data
- Import, export and use of encryption techniques are in compliance with the applicable laws and regulations (E.g., IT Act, 2000)
- Users:
 - Keep their private keys strictly confidential
 - Take responsibility for the safety of their private keys

7. Related Policies

- Access Control Policy
- Communications Security Policy
- Information Security Incident Management Policy
- Operations Security Policy

-----End of Document-----

E Waste Policy


SMU-ISMS

Version - 1.1

(SMU, SMIMS, CRH, SMCPT, SMCON, SMIT)

Revision History

S. No.	Ver. No.	Release Date	Prepared by	Reviewed by	Approved by	Reasons for New Release
1	V1.0	01-08-2019	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) MD Venkatesh Vice Chancellor, SMU	ISMS Implementation
2	V1.1	01-07-2022	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) Rajan S Grewal Vice Chancellor, SMU	Periodic Review


 Head IT (SMU)
 Prepared by
SIKKIM MANIPAL UNIVERSITY
 5th Mile, Tadong
 Gangtok, Sikkim, India
 Sikkim Manipal University
 737102


 Registrar (SMU)
 Reviewed by
REGISTRAR
SIKKIM MANIPAL UNIVERSITY
 5TH MILE TADONG
 SIKKIM 737102


 Vice Chancellor (SMU)
 Approved by
Dr. (Lt General) Rajan S. Grewal, AVS
Vice Chancellor (SMU)
Sikkim Manipal University
 Tadong, Gangtok (Sikkim)

1. Table of Contents

1. Introduction	Error! Bookmark not defined.
2. Scope	Error! Bookmark not defined.
3. Roles & Responsibilities	4
4. Definitions	4
5. Do's and Don'ts	6

1. Introduction

Electronic waste, commonly known as e-scrap or e-waste, is the trash we generate from surplus, broken, and obsolete electronic devices such as computers, laptop, printers and other accessories, Electronics contains various toxic and hazardous chemicals and materials that are released into the environment if we do not dispose of them properly.

This policy provides an overview on collection and disposal of the e- waste the university in our day-to-day operation, disposal of obsolete equipment's is increasingly posing a threat to our environment.

2. Scope

This policy applied to all the constituents or Sikkim Manipal University and all key stake holders.

3. Roles & Responsibilities

The owner of this policy is the Head –IT. He will be responsible for the maintenance and updating of this policy document.

Role	Responsibilities
HEAD IT	Creation and update of this policy as per requirement
Registrar, SMU	Review and Approval of this document

4. Definitions:

E waste means waste electrical and electronic equipment whole or in part or in rejects from their usage and repairing process.

Item Categories

- a) Computers -Servers, Desktop Computers (CPU, Monitor, Keyboard and Mouse)
Printers - Printers, Photocopiers, Scanners, All type of cartridges.
- b) Networking- Switches, Routers, Patch Panels, Model, Converters.
- c) Others - fax machines, telephones, cordless, cellular phones.

- d) Accessories – TV Tuners box, Floppy, CD, DVD, Pen Drives, External HDD, VC Equipment’s.
- e) Electricals Associates – UPS, Power Cables, data cables etc.

E WASTE POLICY

The lifecycle of all IT Assets spanning from acquisition to disposal shall be managed in a manner which confirms to sound environmental norms as detailed in E waste guidelines.

E-waste Guidelines

- I. Preferential dealing with IT Vendors having sound E-waste management processes.
- II. Extending the useful life of IT Asset to postpone / minimizing generating of e-waste.
- III. Responsible disposal processes confirming to regulatory requirements and best practices.

Regulatory Requirements

- I. Head IT will scan the evolving code of practice and keep updating this policy document in line with the best practice for disposal of IT E-waste. This will be done once a year or more frequently if deemed necessary.
- II. The appropriate government bodies have initiated the process approving and authorizing e-waste recyclers, IT Head shall identify authorized recyclers, publish a list of such e-waste disposal.
- III. The list of authorized recyclers and the agreed terms and conditions will be circulated to the purchase & disposable committee.

IT E-waste minimization process

- a. IT shall be endeavor of every user to maximize utilization of all IT Assets to their full productive life.
- b. Apart from internal re-use, option to extend use outside the SMU through donation to Bonafede philanthropic institutions will also extend the useful life of IT Asset.
- c. Only Such Asset which are non-operational and cannot be reused for any other alternate purpose should be considered as IT E-waste for disposal. The disposal committee will certify this position.

5. Do's and Don'ts

DO'S

- Ensure that only Authorized Recyclers repair and handle your electronic products.
- Always call our E-waste Authorized Collection centres / points to dispose products that have reached end-of life.
- Always drop your used electronic products batteries or any accessories when they reach the end of their life at your nearest Authorized E-waste collection centres point.
- Always disconnect the battery from product and ensure any glass surface is protected against breakage.
- Ensure that Data Storages are properly scratched, and no official data must be residing on such devices which should be recoverable in the future to ensure data security.
- Re-usable spares must be separated from the rest of the e-waste before disposal.

DONT'S

- Do not dismantle your electronic products on your own.
- Do not throw electronics in bins having "Do not Dispose" sign.
- Do not give E-waste to informal (Kabaddi) and unorganized sectors like Local Scrap Dealer Rag Pickers.
- Do not dispose your product in garbage bins along with municipal waste that ultimate reaches landfills.

-----End of Document-----

Email Use Policy


SMU-ISMS

Version - 1.1


(SMU, SMIMS, CRH, SMCPT, SMCON, SMIT)

Revision History

S. No.	Ver. No.	Release Date	Prepared by	Reviewed by	Approved by	Reasons for New Release
1	V1.0	01-08-2019	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) MD Venkatesh Vice Chancellor, SMU	ISMS Implementation
2	V1.1	01-07-2022	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) Rajan S Grewal Vice Chancellor, SMU	Periodic Review


 Head IT (SMU)
 Prepared by
SIKKIM MANIPAL UNIVERSITY
 5th Mile, Tadong
 Gangtok, Sikkim, India
 Sikkim Manipal University 737102


 Registrar (SMU)
 Reviewed by
REGISTRAR
SIKKIM MANIPAL UNIVERSITY
 5TH MILE TADONG
 SIKKIM 737102


 Vice Chancellor (SMU)
 Approved by
Dr. (Lt General) Rajan S. Grewal, AVS
Vice Chancellor (SMU)
Sikkim Manipal University
Tadong, Gangtok (Sikkim)

1. Table of Contents

1. Introduction	Error! Bookmark not defined.
2. Purpose	Error! Bookmark not defined.
3. Statement of Policy.....	4
4. Scope	4
5. Administration, Review, and Approval	10

1. Introduction

Electronic mail (email) is a primary means of communication both within the University of Rochester and externally. It allows quick and efficient conduct of business, but if used carelessly or unlawfully, it carries the risk of harm to the University and members of its community.

2. Purpose

The purpose of this policy is to describe the permitted uses of university email. Sikkim Manipal University recognizes the need for electronic communication, specifically email. The University uses Ms Office365 email addresses to officially communicate with students, faculty, and staff. Thus, it is the account holders' responsibility to read, respond and comply with any official university email. Sikkim Manipal University expects all email users to uphold the Mission and Vision and maintain a certain standard of dignity and respect when sending emails.

3. Statement of Policy

Sikkim Manipal University's employees are encouraged to make appropriate use of email for job-related activities that further the University's mission and goals. Sikkim Manipal University students are encouraged to make appropriate use of email for academic purposes and understand this is the official way for the academic administration and employees / faculty will communicate with students. Students / Employees of the University cannot **use University's** email for commercial purposes, personal financial gain, to support a political candidate or movement, or for any unauthorized purpose.

4. Scope

This policy applies to everyone who is provided email services managed by or for the Sikkim Manipal University including, but not limited to, University faculty and visiting faculty, doctors, staff teaching / non-teaching, students, contractors, consultants, volunteers, and guests, any one of which being referred to as a "user" in this policy.

A. Use of Email Accounts

1. University Employees

Email services are intended to allow all University faculty and staff to conduct University business. Personal use of email is not prohibited, provided that personal use

1. Does not materially interfere with performance of an employee's work responsibilities,
2. Does not interfere with the performance of the University networks and
3. is otherwise in compliance with this and other IT policies.
4. High Risk data transmitted by e-mail or other electronic transmission, must be encrypted, or otherwise adequately protected.
5. Protection is necessary for the University or its affiliates to meet compliance obligations, or the unauthorized disclosure, access, alteration, loss, or destruction of those data could have a material impact on the University or its affiliates' mission, assets, operations, finances, or reputation, could pose material harm to individuals.
6. Data are classified as High Risk when protection of such data is required by law or regulation.

2. Students

Sikkim Manipal University currently provides email services to all students. Student use of email is subject to the student conduct codes, as well as this Policy, the University's Information Technology Policy, and the University's Acceptable Use Policy.

3. Ownership of Email Data

Sikkim Manipal University owns all 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.

B. Official Email Address

Students and University workforce members will be assigned an Official Email Address, which will include a mailbox assigned to one of the Official University email systems:

- *University Office 365*

Note: currently Sikkim Manipal University is using in all the constituents Microsoft Office 365 cloud hosted email solution for catering the email requirements.

- The Official University Email Address is the email address that is provisioned upon entry to the University. The Official Email Address is to be used for all University Email correspondence, for populating lists for classes, and for the official online directory. Official communications from university Offices, such as the Vice Chancellors' office, Dean's office, Human Resources, the Finance, and others etc.
- Email services should be provided only while a user is employed by or enrolled at the University. Exceptions may be granted for conditions such as email extensions for emeritus status, researchers transferees etc.

Note: Email services may be terminated with notice if the University determines continuation of services is not in the University's best interest.

1. Use of Email Address to populate University Managed IT Systems

The Official University email address will be the email used to populate any University Managed IT System where "email address" is necessary for the effective business process operation of the system.

2. Use of Email Address as an authentication method for Cloud based services.

The Official University email address will be the email used as the authentication credential for university office365 cloud-based services where email address is the internal authentication method for the service.

3. Email Aliases

The University allows email aliases for the official Sikkim Manipal University email address. For this policy, the email alias does NOT take precedence over the Official University email address.

C. Email Forwarding

1. Manually forwarding University Email that contains information classified as University High Risk is only permissible for valid business purposes and when done using appropriate security precautions.
2. Automation tools, protocols, or rules to enable auto-forwarding (POP, IMAP etc.), to move email from a university managed Email system to a non-University managed email system is not permissible without a formal exception Approval / Permission from the SMU competent authority.
3. Personal email accounts or servers set up to receive or transmit University-related business messaging is not permissible without a formal exception Approval / Permission from the SMU Competent Authority.

D. Confidentiality, Security, and Privacy

1. The password associated with an Email account may be used to authenticate identity in other University online services.
2. To safeguard the user's identity and privacy and the confidentiality of sensitive third-party information stored in email accounts and devices assigned to the user by the University and other University systems accessible using the email password, a user must not share their account or give their password to anyone.
3. Subjecting confidential information to disclosure by sharing a user's password is a violation of university policy and may result in a violation of law and/or breach of contracts to which the University is a party.
4. Users are required to promptly change their Email password upon receiving credible evidence that their password has become known by or disclosed to another party and/or when requested to do so by University IT Team.

5. Although the University does not monitor email content routinely but In certain cases, it may be necessary for the university's IT Team or other University officials to access certain email accounts in the interest of the University's integrity, however users must not assume that Email content will remain private and confidential.
6. A user's expectation of privacy in emails is defined and limited by the University's Information Technology Policy.
7. Access to Email by anyone other than the user may be permitted as described in that policy or otherwise required by law. In addition, Email can be altered or forwarded by a recipient without the sender's knowledge and may also be discoverable in litigation or may be disclosed to comply with a subpoena.
8. Microsoft retains the right to access the O365 Accounts for violations of its Acceptable Use Policy, or in response to subpoena or National Security Letter. (<http://www.microsoft.com/online/legal/v2/?docid=13&langid=en-us>).
9. Faculty and Staff: Employees are discouraged from forwarding any SMU emails to a personal account. Due to the nature of our business, all academic information, proprietary business information or confidential information shared with any employee, is not to be forwarded or shared to any outside entity.

E. Misuse

1. Email is a communication technology. Any policy of the University that applies to communications also generally applies to email.
2. Use of Email in violation of other University policies is also a violation of this policy. See the Use Policy for more details.
3. Use a **non-SMU email** account to link to all personal financial or online account/websites of any kind, or to communicate with others about non university business.
4. The use of email for any of the purposes listed below is prohibited:
 - An infringement on another's copyright, patent, or other property right.
 - Violates, or encourages the violation, of human rights, federal or state laws.
 - A malicious, unlawful, or fraudulent email designed to hack accounts.
 - Includes or promotes any inappropriate content, including, but not limited to, pornography, illegal drug promotion or any gang or illegal activity.
 - Is excessively and inappropriately violent.

- Poses a risk to the public health or public safety of any individuals.
- Using, or attempting to use, accounts of others without permission, including, but not limited to, collecting email addresses and names without the consent of those individuals.
- Concealment or misrepresentation of names or affiliations (e.g., misrepresenting oneself as another user).
- Use of University email to send spam.
- Alteration of source or destination address of email.
- Use of email for partisan political or lobbying activities.
- Use of email for commercial activities or personal gain.
- Use of email to violate the University's policy on Harassment and Discrimination.
- Use of email to violate the law.

F. Spam & Phishing

1. Definitions

- **Spam** is defined as unsolicited and undesired advertisements for products or services sent to a large distribution of users.
- **Phishing** is defined as the attempt to acquire sensitive information such as usernames, passwords, or credit card details (and sometimes, indirectly, money), often for malicious purposes, by masquerading as a trustworthy entity in an electronic communication.
- All incoming email is scanned for viruses, phishing attacks, and spam. Suspected messages are blocked from the user's inbox.
- Due to the complex nature of email, it is impossible to guarantee protection against all spam and virus infected messages.
- It is therefore incumbent on everyone to use proper care and consideration to prevent the spread of viruses and other malware.
- In many cases, viruses or phishing appear to be sent from a friend, coworker, or other legitimate source. Users should not click links or open attachments unless they are sure of the nature of the message. If any doubt exists, the user should contact the IT Team.

G. Retention and Disposal

Users should avoid retaining large amounts of email (whether in the Inbox, Sent Items, Deleted Items, or personal folders) for long periods of time. The University's Policy on Retention of University Records makes clear that Email box is not an appropriate place to retain University records; records that are in a user's Email should be removed to

other paper or electronic storage media intended for archival purposes. Microsoft currently limits each email box to a maximum of 100 gigabytes. Microsoft reserves the right to change this store limit, with prior notice to the University.

H. Sanctions

Violations of this Policy will be handled under normal University disciplinary procedures applicable to the relevant persons or departments. In addition, a violation may result in:

1. Suspension, blocking, or restriction of access to information and network resources when it reasonably appears necessary to do so to protect the integrity, security, or functionality of university resources or to protect the University from liability.
2. Disciplinary action up to and including separation from the University.
3. Department being held financially responsible for the costs incurred as result of a data breach, loss or illegal disclosure.
4. University reserves the right to seek any remedy allowed by applicable law against any individual who, in connection with the use of University Email services or related University electronic resources, intentionally or in the exercise of gross negligence causes material loss or damage to the University or any third party to whom the University owes a duty of care.

5. Administration, Review, and Approval

1. Administration of this policy is assigned to the University IT Department.
2. The head of Information Technology is responsible for reviewing this policy periodically and may incorporate amendments as per the need of the University with the validation and final review from Registrar of the SMU and approval from the Vice Chancellor of the Sikkim Manipal University.

-----End of Document-----

Acceptable Use of IT Resources Policy

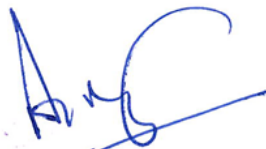
SMU-ISMS Version - 1.1

(SMU, SMIMS, CRH, SMCPT, SMCON, SMIT)



Revision History

S. No.	Ver. No.	Release Date	Prepared by	Reviewed by	Approved by	Reasons for New Release
1	V1.0	01-08-2019	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) MD Venkatesh Vice Chancellor, SMU	ISMS Implementation
2	V1.1	01-07-2022	Anand Ruhela Head -IT	Dr K.S. Sherpa Registrar, SMU	Lt. Gen. (Dr) Rajan S Grewal Vice Chancellor, SMU	Periodic Review


Head IT (SMU)
Prepared by
SIKKIM MANIPAL UNIVERSITY
5th Mile, Tadong
Gangtok, Sikkim
Sikkim Manipal University
737102


Registrar (SMU)
Reviewed by
REGISTRAR
SIKKIM MANIPAL UNIVERSITY
5TH MILE TADONG
SIKKIM 737102



Vice Chancellor (SMU)
Approved by
Dr. (Lt. General) Rajan S. Grewal, AVS, IAS
Vice Chancellor
Sikkim Manipal University
Tadong, Gangtok (Sikkim)

Table of Contents

1. Policy Statement.....	Error! Bookmark not defined.
2. Application of Policy.....	Error! Bookmark not defined.
3. Policy Definitions.....	4
4. Policy Responsibilities	4
5. Enforcement	10

1. Policy Statement

The Sikkim Manipal University provides information resources for employees, students, faculty, and authorized individuals to use in conducting official University business for catering daily activities as per roles and responsibilities assigned.

2. Application of Policy

This policy applies to all users granted access to University Information Resources, including but not limited to students, faculty, teaching & non-teaching staff, and guests.

3. Policy Definitions

A. Access

“Access,” in this policy, means the physical or logical capability to view, interact with, or otherwise make use of information resources.

B. Sub Domain for Email.

“Sub Domain for Email,” in this policy, means the part of an email address that is used to create a secondary name associated with the institution to which the email is assigned or owned, e.g., “smims” is the sub domain in “@smims.smu.edu.in.”

C. Cloud Service

“Cloud Service,” in this policy, means a service made available to a user by a third-party provider via the Internet in an externally managed data center or computing facility.

D. Confidential Information

“Confidential Information,” in this policy, means information that must be protected from unauthorized disclosure or public release.

E. Data

“Data,” in this policy, means all information, regardless of size or storage media, including email messages, system logs, and software (commercial or locally developed).

F. Email Domain

“Email Domain,” in this policy, means the name used in an email address that identifies the University to which the email is assigned or owned.

G. Employee

“Employee,” in this policy, means an individual who is employed full-time, part-time or in a temporary capacity as faculty, staff, or who is required to be a student as a condition of employment.

H. Information Resources

“Information Resources,” in this policy, means the procedures, equipment, and software employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information.

I. Information Owner

“Information Owner,” in this policy, means a person with operational authority for information who is responsible for authorizing controls for generation, collection, processing, access, dissemination, and disposal of that information.

J. Least Privilege

“Least Privilege,” in this policy, means the security principle that requires the application of the most restrictive privileges needed for performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

K. Personally Identifiable Information

“Personally Identifiable Information,” in this policy, means information that alone or in conjunction with other information identifies an individual, including an individual’s name, social security number, date of birth, or government-issued identification number; mother’s maiden name; unique biometric data etc.

L. Primary Email Domain

“Primary Email Domain,” in this policy, means the name used at the end of an email address that identifies the name of the organization to which the email is assigned or owned, e.g., “@smu.edu.in”.

M. Users

“Users,” in this policy, means individuals or automated applications that are authorized to access information or information resources in accordance with the information owner- defined controls and access rules.

4. Policy Responsibilities

A. Guidelines

The following guidelines set out the permissible use of Sikkim Manipal University Information Resources:

1. Authorized Use

Individuals may use University Information Resources for the purpose of conducting University business or as otherwise set out in this policy.

- a. The University may limit the use of Information Resources to specific research, teaching missions, administrative, financial transactions, or other purposes at its sole discretion, and may otherwise restrict or revoke authorization at any time.
- b. University students may use University information resources for institutions- related and personal purposes in accordance with this policy and other applicable University policies, provided personal use does not result in any additional costs to the University.
- c. University employees teaching & non-teaching and authorized individuals may use Information Resources in accordance with this policy and other applicable University policies and in accordance of IT Act 2008 , Incidental personal use of Information Resources by employees and authorized individuals is permitted, subject to review and reasonable restrictions by the employee's reporting authority or competent authority of the university, provided the use does not interfere with the performance of job responsibilities and does not result in any additional costs to the University or breach of confidentiality of sensitive information to the external agency
- d. The University may provide Information Resources access to the employees transferred on deputation to the other group institutes, visiting scholars, external examiners, vendors, and other external users as necessary to advance the mission and operation of the University / CRH Hospital. Information Resources must be used in accordance with this

policy, any contractual obligations in accordance to the agreement and maintaining the confidentiality of the business information.

2. Freedom of Expression

University information resources are a non-public forum unless otherwise expressly designated by the appropriate University official. The University will not restrict access to information through its Information Resources based on content or viewpoint if the information meets legal standards. However, the University reserves the right to limit, restrict, or deny Information Resource privileges or access for those who violate the University policies.

3. Privacy

Users of University Information Resources have no expectation of privacy regarding information collected, recorded, processed, stored, displayed, retrieved, or transmitted using University Information Resources beyond that which is expressly provided by applicable privacy laws. The University may monitor, access, and review any such information for university purposes or duties. This information also may be subject to review or disclosure in accordance with the following:

- a. Breach of Confidentiality of the sensitive information and sharing the information without permission / approval from competent authority of the Sikkim Manipal University.
- b. administrative review for security or compliance purposes.
- c. computer system maintenance.
- d. law enforcement and other investigations.
- e. audits; and as otherwise required to protect the reasonable interests of the University and other users of Information Resources.

The University does not guarantee the protection of electronic files, data, or other information, including e-mails, from unauthorized third-party access.

4. Intellectual Property

Any development works files, software, piece of data, mobile app, source code for business application being used to facilitate automation for the academic purpose has been created or communicated through University Information Resources are subject to university copyright policy and applicable copyright laws. University Information Resources may not be used to violate intellectual property rights, including downloading or distributing copyrighted material without proper authorization from the competent authority of Sikkim Manipal University.

5. Valuable Assets

Information Resources purchased or leased by the University are the property of the University or the vendor from whom the resource is leased. Any unauthorized access, use, alteration, duplication, destruction, or disclosure of these assets may be a criminal offense as per the IT act.

6. Transportation
University Information Resources and data contained in the Information Resources may not be transported domestically or internationally without appropriate authorization, including authorization required from competent authority of Sikkim Manipal University or HOI of respective institutions.

B. Information and Technology Use

1. Security
 - a. The use of Information Resources and data must comply with the Information Security Policy of Sikkim Manipal University, the SMU IT System Information Security, and applicable information security standards and privacy policies. Access, usage, and treatment of Information Resources and data must not violate the confidentiality, integrity, or availability of these assets, and must adhere to the principle of least privilege to ensure that access is assigned as appropriate for tasks that are to be performed and removed when no longer necessary.
 - a. Retirees / contractual, visiting scholars, vendors and other external users may obtain access to Information Resources based on their role.
 - b. Access and use of data must be approved by the information owner prior to use, processing, and installation.
 - c. University Information Resources and data must be encrypted if transported domestically or internationally duly approved from competent authority of the SMU.
 - d. Upon termination, retirement, change in employment status, or cessation of an agreement or contract with the University, access to Information Resources and data must be terminated or modified in accordance with the new status of the individual. University-owned accounts, data, email, and Information Resources that were assigned to or used by a former employee, visiting scholar, vendor or other external user must be recovered and transferred to the former employing or hosting department for business continuity purposes.

2. Email Use

- a. Email is the mechanism by which the University officially communicates with employees and students and external stakeholders. Only email systems authorized by IT Shared Services may be used to send email communications on behalf of a university email domain. Third-party senders may not create an appearance that email sent by the official University correspondence. Automatic forwarding of bulk email to a third-party email system or third-party email address is prohibited.
- b. Email should not be used to store or transmit personally identifiable or confidential information to external parties unless the email is encrypted or secured in accordance with applicable University policies and Cyber Security standards.
- c. Content contained within an employee's mailbox remains under the custody of the employing department and will be retained by the department when an employee separates from the department, or when a change in employment status occurs. It is the responsibility of a department to archive email contained in the mailbox of a former employee or a retired employee for business continuity purposes.

3. Cloud Services

The use of cloud services must be compliant with University policies and applicable Cyber Security policies, privacy, procurement, administration, supplier service relationships, export controls, and appropriate use of Information Resources and data.

University data may not be transmitted, processed or stored by a third party until Information Security and the appropriate IT groups have conducted a security assessment and approval / permission obtained from competent authority of SMU. Cloud service providers must ensure the confidentiality, integrity and availability of data, information, and services that they provide.

4. Websites

Website usage and web administration must comply with university policies, standards, and applicable laws, including those that address web accessibility, security, and privacy.

5. Personally Owned Accounts, Software and Contracted Services

Personally owned accounts, software, and contracted services may not be used to conduct university business, including transmission, storage, or processing of data that is owned by the University.

6. Network Access

IT Shared Services is responsible for ensuring that networks are administered in a manner that facilitates availability to all users. Only authorized devices may connect to university networks. The introduction of devices or information resources that negatively affect the behavior or security of the network, or violate University policies, is prohibited.

7. Remote Access

Users that remotely access University information resources from an external location must ensure that information resources used at the remote location comply with the SMU Information Security Policy, including the requirements that address secure network and access control mechanisms, secure exchange of information transferred between the remote location and the University through use of the University VPN, current maintenance of information resources, and prevention of unauthorized viewing of confidential and personally identifiable information.

C. Responsibilities

1. IT Security / Cyber Security and safety of IT resources is the responsibility of every user.
2. Users shall use University Information Resources responsibly, respecting the needs of other Users.
3. Users are responsible for any usage of his or her account, Information Resources or data entrusted to him or her.
4. Users must maintain the secrecy of their passwords. If a user suspects their password is compromised, they must reset it with all complexity as per password policy, as soon as possible.
5. Users must report any misuse of Information Resources or violations of this policy to their Head of the department, HOI, HOU or Head of IT.
6. Users are responsible for obtaining and adhering to relevant Information Resources policies.
7. Users must comply with IT Policy, revised IT Act 2008, IT regulations, contractual agreements, institutional regulations and policies, licensing agreements and defined procedures.

8. Users are responsible for reporting security incidents, including any potentially compromised accounts, suspected system irregularities, and/or vulnerabilities, to the SMU /SMIT IT team or Head IT.
9. Users must use Information Resources only for the purpose in which access has been authorized and only in the manner and to the extent authorized. The ability to access Information Resources does not, by itself, imply authorization to do so.
10. HR Department is responsible for promptly informing University officials and information technology personnel when employment status changes occur, and when written agreements or contracts with visiting scholars, vendors, or other external users terminate to ensure that access to Information Resources are disabled or modified as appropriate.

D. Misuse of Information Resources

The following actions constitute misuse of the University's Information Resources and are strictly prohibited for all Users:

1. Use of University Information Resources in support of or for illegal activities. Any such use will be reported to the appropriate University official. Head IT, HOI, HOU of respective institutions. Criminal and illegal use may involve, but is not limited to, unauthorized access, intentional corruption or misuse of Information Resources, theft, obscenity, and pornography.
2. Failure to comply with laws, policies, procedures, license agreements, and contracts that pertain to and limit the use of the University's Information Resources.
3. Abuse of Information Resources, including, but not limited to:
 - a. any act which endangers or damages specific software, application, source code, hardware, program, network, or system as a whole, whether located on campus or elsewhere on the global Internet.
 - b. creating or purposefully allowing a computer malfunction or interruption of operation.
 - a. injecting a virus or other malware into an Information Resource.
 - b. sending a message with the intent to disrupt University operations or the operations of outside entities.

- c. sending spam messages.
 - d. computing tasks that consume an unreasonable number of resources, either on or off campus, to the detriment of other authorized users; and
 - e. failing to adhere to usage limitations that apply to computer facilities on campus.
4. Use of University Information Resources for personal financial gain unrelated to University responsibilities and job expectations or for a personal commercial purpose.
 5. Failure to protect the privacy of a password, account or confidential information from unauthorized use or access.
 6. Permitting someone to use another's account or credentials or using someone else's account or credentials.
 7. Unauthorized use, access, reading, or misuse of any electronic file, program, network, or system.
 8. Unauthorized use, access, duplication, disclosure, alteration, damage, misuse, or destruction of data contained in any electronic file, program, network, or University hardware or software system.
 9. Unauthorized duplication and distribution of commercial software and other copyrighted digital materials. The unauthorized duplication and distribution of software and other materials created for the University (including academic application, software, or software's source etc) is a violation of copyright law and this policy. Exceptions to this violation include the act done with written permission / approval from competent authority of Sikkim Manipal University by specific authorization.
 10. Infringing upon the copyright, trademark, patent, or other intellectual property rights of others using institutionally owned Information Resources.
 11. Attempting to circumvent, assisting someone else, or requesting that someone else circumvent any security measure or administrative access control that pertains to university data or Information Resources.
 12. Use of University Information Resources in a manner that violates other University policies.
 13. Use of University Information Resources for the transmission of commercial or personal advertisements, solicitations, or promotions.

14. Use of University Information Resources for transmission of political material.
15. Installing unauthorized software or hardware that permits unauthorized access to institutionally owned information and Information Resources.

E. Access to University Information Resources

The IT Team of IT administrators of University Information Resources must provide University faculty, staff, students, and other individuals access to University Information Resources in accordance with this policy when such access is appropriate to the individual's role or function at the University.

F. Disciplinary Actions

Failure to adhere to this policy may lead to the cancellation of the individual's account(s) and to other disciplinary action by the University Committee. Additionally, individuals may be subject to possible civil and criminal action in accordance with the nature of the breach of violation of the Policy or revised IT Act 2008 as per the GOI / GOS.

5. Enforcement

This policy will be reviewed and revised from time-to-time based on business and (or) technological requirements and the same shall be published as revised versions. Any deviation from the above policy should be documented, approved, and signed by Head IT.

Related Policies

- Access Control Policy
- Information Asset Management Policy
- Communication Security Policy
- Human Resource Security Policy
- Information Security Incident Management Policy
- Operations Security Policy
- Organization of Information Security Policy
- Physical and Environmental Security Policy

-----End of Document-----