SANGAM UNIVERSITY IT POLICY

Sangam University provide all Faculty members, students and staff with a modern, fully networked computing and IT environment for academic use. Users of Sangam University Bhilwara computing, networking and IT facilities are expected to abide by the following rules which are intended to preserve the utility and flexibility of the system, protect the privacy and work of students and faculty, and preserve our right to access the international networks to which the system is connected. In case of complaints, appropriate action to be taken will be decided and taken by the competent authorities.

Computer Usage:

- The purpose of University policies regarding computer and network usage is to protect all individuals affiliated with Sangam University.
- Inappropriate use exposes the University to risks, including virus attacks, compromise of network systems and services, and possible legal liability.
- Access to the information technology environment at Sangam University is a privilege and must be treated as such by all users.
- Students are expected to be positive members of the University community, which extends to cyberspace, by following the Community Code and all University policies.
- Users who violate any acceptable use policy will be subject to disciplinary action, up to and including loss of privileges and/or expulsion, and may be at risk for civil or criminal prosecution.
- All violations will be handled in accordance with Sangam University policies and procedures.
- While it is our intent to maintain a creative and educational environment, please be aware that all equipment and functions related to the operations of the computer systems at Sangam are university owned. Please also be aware that no expectation of privacy should exist for any material stored on the computer network or computer equipment.

Following is a brief summary of relevant University policies regarding computer and network usage. All policies in their entirety can be found on the University's website.

Faculty, staff, and students with authorized accounts may use the computing and IT facilities for academic purposes, official University business, and for personal purposes so long as such use

- Does not violate any law, University policy or IT act of the Government of India.
- Does not interfere with the performance of Sangam University Bhilwara duties or work of an academic nature.
- Does not result in commercial gain or private profit other than that allowed by the Sangam University Bhilwara.

Acceptable Use Policy:

- Sangam University information technology resources, including electronic communications on and off the SU campus and the computers attached to this network, are for the use of persons currently affiliated with Sangam University, including faculty, staff and students.
- Information technology resources are provided by the University to further the mission of lifelong education. Use of these resources should be consistent with this mission and this policy. Central to appropriate and responsible use is the stipulation that computing resources shall be used in a manner consistent with the instructional, public service, research, and administrative objectives of the University.
- Use should also be consistent with the specific objectives of the project or task for which such use was authorized.
- All uses inconsistent with these objectives are considered to be inappropriate use and may put at risk further access to services.

Unacceptable Use Policy:

- Using the resources for any purpose that violates Sangam University or state laws.
- Using the resources for commercial purposes, sales and/or advertising.

- Using excessive data storage or network bandwidth in such activities as propagating of "chain letters" or "broadcasting" inappropriate messages to lists or individuals or generally transferring unusually large or numerous files or messages.
- Sending or storing for retrieval patently harassing, intimidating, or abusive material.
- Misrepresenting your identity or affiliation in the use of information technology resources.
- Using someone else's identity and password for access to information technology resources or using the network to make unauthorized entry to other computational, information or communications devices or resources.
- Attempting to evade, disable or "crack" password or other security provisions of systems on the network.
- Reproducing and/or distributing copyrighted materials without appropriate authorization.
- Copying or modifying files belonging to others or to the University without authorization including altering data, introducing or propagating viruses or worms, or simply damaging files.
- Interfering with or disrupting another information technology user's work as well as the proper function of information processing and network services or equipment.
- Intercepting or altering network packets.

Mailbox Management Policy

Sangam University e-mail account is permitted for official communication which is created on the basis of E-Mail ID/ Internet ID Request Form. To establish guidelines for automatic removal of older mail items in the Inbox, Sent Items, Calendar, and Deleted Items folders, automatic removal will maintain the client databases, limit disk space usage, and reduce possible corruption. Reasonable mailbox sizes are allotted to efficiently manage the universities email system.

The email account is set up so that following system is automatically implemented as follows:

Inbox - In order to maintain mail users may establish automatic archiving to a specific directory on your personal computer or within another folder in your mailbox before the dates indicated above. Please reference HELP in the particular email client for assistance.

This policy covers appropriate use of any email sent from Sangam University email address and applied to all employees, vendors, and agents operating on behalf of Sangam University.

The Sangam University email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, religion, or national origin.

Employees who receive any emails with this content from any Sangam University employee should report the matter to web administrator. All email sent or received from a Sangam University server must comply with the Acceptable Use Policy.

File Sharing Policy

- The purpose of this policy is to define Sangam University's position on the sharing, distributing, or using illegal or unauthorized copies of software, music, video, and all other forms of piracy; digital or non-digital.
- The individual with primary responsibility is the Network Administrator.
- Providing or obtaining unauthorized copies of audio and visual works in either digital or non-digital format is not appropriate and may be illegal.
- Any number of file-sharing must be done through local server or university mail account.

Copyright Law

- Sangam University takes a strong stand against unlawful distribution of copyrighted music, movies and software.
- If a faculty/student is found to be distributing copyrighted material using any university computing resources, that person's network connection will be terminated and the person will be referred to the Sangam University Authorities for further action.
- If the user provides or obtains copyrighted files (music, videos, text, etc.) without permission from the copyright owner or their representative or system administrator, the user is in violation of state copyright laws and the Sangam University Acceptable Use Policy.
- Use of copyrighted software for teaching and learning process by individual users under the guidance of competent authority is permissible.

Network Service

- Sangam University routinely monitors network usage patterns to check any possible interference with the ability of others to use the network services which violates University policy and may result in termination of access to the university network services, and other disciplinary action.
- Categories for internet usages are defined as per **annexure-1**.

Network Use Policy

- To establish guidelines governing the use and connection of networking devices on the University's Communications Network. This policy applies to all university networked devices, ranging from multi-user systems to single user personal computers. This includes networked printers, mini-hubs, routers, switches, and any other network communication devices, which are connected to the university's network. The individual with primary responsibility is the Network Administrator and the back-up designee.
- The university provides network access and capabilities through the Unified Threat Management. The guidelines listed below are required in order to provide the university a reliable and stable networking platform.
- All networking equipment connected to the university network must first be registered and approved by Network Administrator. The responsible parties with problem network devices and/or services will be notified and expected to correct the problem in a timely manner.
- Any networked devices or services that degrade the quality for service on the network, will result in termination of network service to that device until the correction occurs. Activities, which interfere with the operation of the network, are prohibited. These include but are not limited to the propagation of computer worms, network sweeps, network probing, viruses, or Trojan horses.

Data Management

Data Backup, Restoration and Retention

The objective of "Data Backup Policy" is to ensure protection and retention of university data. For the purpose of preventing loss of data, university data is saved regularly onto the back up media or on Data server.

The policy for taking Data Backup is as follows:

The university data pertains to the following categories:

- Server – Blade server(ERP), Towel server, File Server, Data Server,
- Users – Desktop, Laptop.

Server

- The backup of the server will be taken at the location where respective servers are located.
- Every day incremental backup will be taken and every week, full backup will be taken.
- Monthly Backup which is last week of the month will be kept for every month for last 1 year.
- Yearly backup will be kept as per university requirements.
- Tagging of backup will be as per following format:
- <SU> <D Drive > <Backup folder >/<date wise> : >
- The responsibility of backup for the server and backup log book is that of system administrator& ERP Manager.
- Backup media should be kept in a safe Place.
- Competent authorities to provide list of specific Data for specific periods required to be kept either on production servers or through archiving solutions. This list must be maintained by system administrator where the servers are commissioned.
- The backup media after the retention period required to be destroyed must be stored at a predefined location away from the useful media and a log register duly updated must be maintained. This obsolete media must be destroyed at least once every year as per e-waste process

There should a backup/restoration environment for Servers. At present application servers may have techno-commercial constraints to have this environment. New Application Servers to be deployed should have the Backup recovery environment. Once this environment is made available, the system administrator shall ensure periodic restoration of backup data and maintain record of the same.

User's data Backup

Back up of university data files residing on users workstations shall also be taken.

- It is the responsibility of every user to keep these university data files at the designated locations on the common file server, as provided by system administrator, on a regular basis.
- The backup for file server will be taken up as per above process
- If for any reason a backup for critical data needs to be taken up, then a request should be emailed to the system administrator, with approval from reporting competent authorities.
- Backup for the critical desktops/laptops should be taken. These critical desktops/laptops should be identified by department in consultation with respective department Head.

Data Confidentiality

- The functional heads will be responsible for confidentiality of respective university data. Users must not use the IT infrastructure, application and communication systems, whether standalone or in conjunction with any other device, to make an unauthorized disclosure or copy of confidential information belonging to the department /university.

The unauthorized disclosure or copying of information belonging to the university will be liable for appropriate disciplinary action.

Such confidential information shall include without limitation details of:

- Business contacts, associates, lists of customer and suppliers and details of contracts with them.
- Identities of students.

- Sales, expenditure and buying/pricing policies including details of percentage mark-up of profits and discounts.
- Accounts , treading statements , statistical information and other financial reports
- Marketing strategy, admission reports and research results and forecasts.
- Details of the employees and their remuneration and other benefits.
- Presentations, reports, projects, case studies, research, offered or undertaken by the university.

IT Budget

Annual Budget Preparation

- **Department Level:** It is the responsibility of the department Head to prepare the annual budget for IT expenditure at the department Level: Capital and Operational, before the beginning of the financial year with inputs from system administrator. The same should be submitted to system administrator for integration with overall budget for the university. The approved Budget should be communicated to department head.
- **University Level:** It is the responsibility of the system administrator to prepare the budget for IT expenditure (both, capital and operational), at university Level before the beginning of the financial year. The expenditure for university Level initiatives should be submitted to respective department Heads and approval must be taken before the start of the new financial year.

Budget Monitoring

- **Department Level:** It is the responsibility of the purchase Department or Store to monitor expenditure against budget at the Department.
- **University Level:** It is the responsibility of the purchase Department or Store to monitor expenditure at the university level against budget.

Unbudgeted Expenditure

For any agencies or any expenditure pertaining to immediate requirements for IT to cater to major unforeseen issues affecting university operations or for any new un-planned technology.

Security Tools

To enhance security, System Administrator may identify and implement requisite tools, both for external and internal security. To enable better security and identify specific tools, if required, services from specialist partners can be taken.

Other Security Measures

"Write enabled disc"(CD/DVD) drives shall not be provided and shall be removed/disabled from existing users workstation. If there is an occasional need for user to store some information on a disc, necessary approval is to be sought.
Possession and usage of removable media such as: MP3 players or Flash drives, is prohibited. By default, the USB ports of the users should be blocked and depending on requirements, it would be unblocked for selected users with the approval of competent authorities.

System administrators or data/ process owners and fulfill or deny the request as appropriate.

Following passwords structures (Format & Frequency) are to be followed:

Server/ application	Responsibility	Type of password	Frequency of change in password
Blade server(ERP)	ERP manger &System Admin	Alpha-Numeric	45 days
Windows OS	Users	Alpha-Numeric	
Towel server	System Administrator	Alpha-Numeric	45 Days
File Server	Employee	Alpha-Numeric	As per user requirement
Data Server	No User name	NO password	

- User id and password should not be the same.
- The initial user account password will be communicated by the System Administrator. But the password must be changed at first instance while Logging system.
- The password should be known only the individual or a group of users to whom it is assigned and should not be shared with other users (internal or external to the organization) including head or technical staff or non-teaching unless authorized by competent authorities.
- The responsibility of sharing the password lies directly on the user/group. The list of authorized group users must be maintained by system administrator.
- If a password is suspected to be compromised, then the password should be changed immediately and the same should be informed to department head.
- Wherever applicable, account Lockout threshold should be implemented with (5) attempts i.e. User accounts will be locked automatically after five unsuccessful password attempts. If this happens, the users should contact to system administrator their account with appropriate reason for account lockout.

Violations of this policy will be handled in accordance with Sangam University policies and procedures.

Following set of rules will applicable to new joining or someone who is getting relived from the university.

A. EMPLOYEE JOINING

1. **Mail Account Policy**

- On the joining of new employee, HR department will handover **IT Resources Requisition Form (Annexure-1)** get it filled from new joining.
- HR department then handovers IT Resources Requisition Form to Web administrator for further action.
- Web administrator will generates new Mail Account and send password to employee personal mail account with IT policy of Sangam University.
- Web administrator is also responsible for uploading faculty detail on Sangam University website.

2. Internet Access Account Policy

- System administrator will generate Internet Access ID on receiving IT Resources Requisition Form.
- System administrator will provide IT resources to employee by the instruction of competent authorities.
- System administrator will send the mail to ERP coordinator for creation of ERP account.
- System administrator is also responsible if any upgradation in allotted IT resources on recommendation of competent authorities.

B. EMPLOYEE RELIEVING

1. Mail Account Policy

- When employee is to be relieved this university HR department issue No-Dues certificate to employee.
- Employee takes a sign of web administrator on that form.
- Web Administrator will suspend mail account of that employee or recommend to competent authorities for future access.
- Web administrator will remove name of employee from different mail account groups.
- Web administrator will remove detail of employee from Sangam University website or by the permission of competent authorities.

2. Internet Access Account Policy

- When employee is to be relieved this university HR department issue No-Dues certificate to employee.
- Employee takes a sign of system administrator on that form.
- System Administrator will be responsible for deactivating the account Access or ask to competent authorities.
- System administrator will send the mail to ERP coordinator for deactivation of ERP account or by the permission of competent authorities.
- System Administrator will takes back all IT resources issued at the time of joining.

Hardware Purchase Policy

- Requirement of Equipment come from university departments with permission of competent authorities.
- System Administrator will put this requirement to store for further process.
- Store accepts this requirement and asks vendors for the quotation.
- Minimum two quotations and maximum 4 quotations are acceptable.
- Store prepares summary sheet and put best quotation to competent authorities for approval.

For Software Purchase Policy

- Requirement of Equipment come from university departments with permission of competent authorities.
- System Administrator will put this requirement to store for further process.
- Store accepts this requirement and asks vendors for the quotation.
- Minimum two quotations and maximum 4 quotations are acceptable.
- Store prepares summary sheet and put best quotation to competent authorities for approval.

For Software /Hardware Renewal Policy

- Renewal of hardware and software on specific date by the permission of competent authorities.
- System Administrator put this requirement to store for further process.

- Store accepts this requirement and asks vendors for the quotation.
- Minimum two quotations and maximum 4 quotations will accept.
- Store prepare summery sheet and put best quotation to competent authorities for approval.

Annexure-1

IT Resources Requisition Form

Date: _____

For Use of HR

Name	_____	_____	_____
Employ Code			
Designation			
Department			
Personal Email ID			
Contact no			

For use of Web Administrator

Assigned official mail Id:	_____@sangamuniversity.ac.in
Assigned User Name (Internet):	_____

For use of System Administrator

Item Name	S. No.	SU S. No.	Remark
Computer System:			
Hard Disk:			
RAM:			
Mother Board:			
Printer:			
Scanner:			
Etc.			

(Employee) (Web Administrator) (System Administrator) (HR)