SXCS/P-10

Enterprise Resource Planning Policy

It is the operational requirement of the College to provide state-of-the-art information systems and electronic communication services (via Internet and Intranet) to enhance the workflow and carry out the administrative activities of the institution effectively and efficiently. For this purpose, the institute has implemented the ERP system.

Everyone with access to the computer and the internal network can use the ERP. This includes the usage of all the software features with necessary authorization. While the ERP is a great resource for the organization, each employee/student is expected to use it responsibly and respectfully.

Security

- The entry and exit points of internet are protected by firewall
- All authorized users are provided with a username and passwordto login into the ERP and access the required portals
- Each user has features defined as per the departmental job roleand requirement

Usage Policy

Access is provided 24/7 for employees and students of St. Joseph's College of Commerce.

Do's

- Additional software features can be requested and are allocated once the relevant authorities/ manager approve the need for it
- All information shall be shared on a need-to-know basis.
- Each user shall be given necessary (and restricted) access to the ERP.It shall be mandatory to follow the access limits strictly.
- The employees shall be held responsible for inappropriate use of information, which they have access to. All passwords must be kept confidential, and computers shall be locked/ logged outfrom, while

they are away

- The institution shall have the right to monitor any/all the aspects of this technology
- The employees shall be required to read and follow the technology updates sent from time to time. These shall include tips for effective use of technology, information security, new technology and upgrades
- All personal greetings, displays or messages on any technology shall be formal and professional

Don'ts

- The employees are expected to not use the institution's technology for personal financial gain or profit
- Carrying information in printed or soft copy shall be prohibited without prior sanction from the manager. No employee shall copy information illegally.
- There shall be no tolerance for the use of technology for any actions that are harassing or discriminatory in nature.
- A breach of any of the above guidelines or not following the policy guidelines shall lead to strict disciplinary action against the concerned employee.
- Technology is linked hence inappropriate use of one aspect of technology can cause unintended consequences in another. An employee shall always consider the availability of resources for others as well as the overall operational efficiency of the technology system.

Software Usage

The institution shall own all software and make it available to employees according to the need, under the terms of licensing agreements between the institution and individual software vendors.

If an employee leaves the institution, any institute-owned software in his or her possession must be returned. To use resources wisely, employees are expected to learn what existing software can do.

External Access

Remote access: Remote Access allows users to access the SXCS ERP resources or data from an external location outside the college premises. This access may be by a third party or an employee who is located off-site. For cost and other security reasons, remote connections must be closed as soon as relevant work is completed.

Third Party Access: Third Party Access to St. Xavier's College resources or data is given to an individual who is not an employee of the college.

Examples of third parties include:

- Software vendor who is providing the technical support
- Contractor or consultant
- Service provider
- An individual providing outsourced services to St. Xavier's College requiring access to applications or data

Third Party Access can only be provided after the Third Party has signed a confidentiality agreement that must be included in their formal contract with SXCS. SXCS staff must never permit another individual to utilize their username to access the SXCS network resources.

Further requirements for granting Third Party Access are:

- Risk analysis process
- Approval by Data Owner
- Approval by the Head of ERP /relevant IT resource

Third party access will only be permitted to facilities and data that are required to perform specific agreed tasks as identified by SXCS in the case that a third party is required to access end customer's data and related resources, relevant approvals must be obtained from the Management.

Backup and Recovery Policy

Backup is done separately and labelled properly. Daily backup of the SQL databases and other important user data (decided by ERP admin) are scheduled at 4.00 a.m.1ST. Procedure is as follows:

- Monday to Sunday complete backup is done. At the end of every month, all backups will be moved to the External Hard Drive. For this,

we have earmarked external drives which will be circulated.

- All the backup devices are labelled and logged for control and disaster recovery measures. ERP Department strictly controls the access to the drives and CD backups.

Misuse of data

Misuse of information systems would cover every action that disturbs the use of information systems for its intended purpose. Causing harm or damage in any data, using characteristics of the systems for its originally unintended purposes are prohibited by the administrators of the information systems.

Prohibited activities on the ERP system, some of which may constitute criminal activity, including (but not limited to) the following:

- Alteration of system software or hardware configurations and data without authorization.
- Information classified as confidential or proprietary must not be sent over the internet, for example: a file transfer, email content, file attachment or via a web session, unless protected by appropriate security measures.
- Unauthorized access to or use of other users' accounts.
- Unauthorized decryption of coded information such as passwords.
- Forgery or attempted forgery of data.
- Generating or forwarding chain letters, or participating in anykind of multilevel or pyramid scheme.
- Storage or transmission of copyrighted materials without the permission of SXCS.
- Attempts to evade or bypass system administration policies, suchas resource quotas, firewall and web filter settings.
- Harassment via impersonation of other users.
- Participate in illegal activities such as making threats, harassment, theft, breaching security measures, or violating anyother applicable law or policy.\
- Uploading or downloading any kind of socially or ethically objectionable material.

Investigation and Consequences of Misuse

All data communication networks are administered by the IT Department. During the investigation, as a process of normal monitoring or on reported incidents, Systems Administrators have the right to prevent or limit the use of information systems. In addition to this, in case of misuse, the following consequences may also be applied:

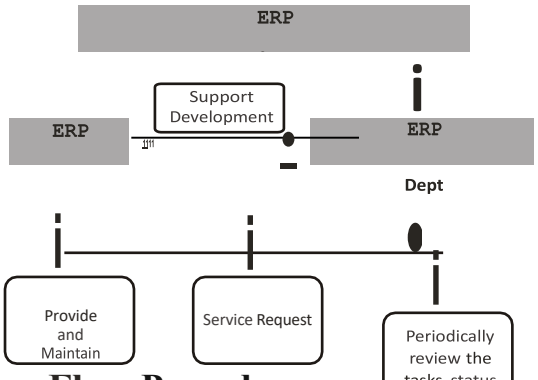
Limitation or denial of usage

Disciplinary action

SXCS at its own discretion will act on any misuse: monitored or reported. In all such circumstances, the institution reserves its right to decide on the services offered to the employees/students and take such necessary action individually or collectively, as may be deemed appropriate by the institute.

Procedure Objectives

The purpose of ERP department is to provide and maintain the software and hardware for the institution and ensure the continual operations to meet the request by the employees/students towards the **ERP.**



Process Flow Procedures

Input	Tasks	Output
Software Requests Permission List Issue Resolution	Service Requests Provide necessary	Software updates Allocate Priority Backup

Request	infrastructure Maintain the	Service Register

J **Entry Criteria** infrastructureJ **Exit Criteria**

New development Requirements Preventive Maintenance Requirement	Plan for Preventive Maintenance Periodically review the tasks status	Approved Preventive Maintenance Plan SLA Analysis Hardware / Software Request Closure

J Verification

- Review of kick-off meeting agenda
- Review of the request reported
- Review of the Software requirements
- Review of the status of pending issues
- Review the Service Level Agreement
- Verification through Periodical Audit

Task Manager

i. Manage Service Requests

a) Raise service requisition for any software breakdowns andsend to the ERP Department. (REQUESTOR)

b) Analyse the service request raised. (ERPADMIN)

- Initiate steps to solve the problem by identifying the type of service. (ERPADMIN)
- Log a complaint with the vendor ifit is a software problem.
- If the service request is under data issues, then log a complaint and distribute it to the Vendor.
- Else the service is addressed in-house.

c) Assign priority to the tasks based on the task category and allocate the tasks to the technicians for task resolution in case i t is in-house maintenance. (ERPADMIN)

a. Track the task completion status and communicate the same tothe Requestor (ERPADMIN)

b. On confirmation from the requestor, update the records withtask status as closed (ERPADMIN)

c. Effective tracking for the SLA will be performed (ERPADMIN)

d. Provide necessary infrastructure

a) Raise a software /hardware requisition form (ERPADMIN)
b) Take approval from concerned stakeholders. (IT Manager /
c) Principal)
d) Submit the approved software/hardware requisition form to the IT Department (ERPADMIN)
e) Verify availability of the stocks and commit the timeline as per SLA for providing infrastructure requirements (ERADMIN)
f) When the requested infrastructure is not available in stock, communicate to the Principal, IT department and Initiate purchase process. (ERPADMIN))
g) Provide the infrastructure to the project after receiving the product from the purchase department. (ERP ADMIN/ Requestor)
h) For an individual's requirement
i) Get the approved (approved by the principal) Software requisition form for individual requirements (ERP-ADMIN/Principal)
j) Provide the requested Software update and close the request (ITM/FH/RE)

ii. Maintain the infrastructure

a) Security (Computer Viruses/ Malware, Software Installations, Laptops, Confidentiality) (ERP ADMIN)
b) Access policy (ERPADMIN)
c) Allow and block External/Internal Access to the ERP (ERPADMIN)
d) Backup and Recovery policy (ERPADMIN)

iii. Plan for Preventive Maintenance

a) Prepare a preventive maintenance plan (once in six months) (ERP ADMIN)
b) Periodically perform preventive maintenance work as per the preventive maintenance plan (ERP ADMIN)

v. Periodically review the tasks status

a) Pre pare the quarterly/ half yearly status report based on the data collected from
b) service request resolution and communicate the same to the

management (ERP ADMIN)

c) Conduct periodical status review meeting and review the statusof pending issues (ERP ADMIN /Principal)

d) Review the SLA compliance level and plan for improvement (ERPADMIN)

e) Revoking of password & handing over important data (ERP ADMIN)

f) Removing of all access privileges of the employee (ERPADMIN)