IT POLICY

Christ University, Bengaluru

Table of Content

IT SERVICE MANAGEMENT

IT Service Management

Purpose

Purpose to implement effective IT Infrastructure management in order to support end users towards effective teaching and learning

Description

IT Service management is automated through various services offered to end users like ERP system, Mail Services and Helpdesk. Support request from various end users have been addressed by implementing resolution duration based on criticality on which priority has been set to resolve the cases in time

Call Management System:

All system related problems to be reported to Help desk In-Charge who shall prioritize the problem reported as per the following priority

Priority Description		
Priority ID	**Description**	**Resolution Duration**
P1	High –P1	1 Hour
P2	Medium –P2	2 Hours
P3	Low –P3	4 Hours
P4	Low – P4	8 hours

P1 - High Priority Departments/Office			
SL.No	**Department**	**Location**	**Resolution duration**
1	Accounts	Central block	
2	Admission	Central block	
3	Directors Cabin	Central block	
4	Exam Office	ALL Blcoks	
5	IPM	Central block	
6	IT-Services	Central block	1 Hour
7	KP - SW division	Central block	
8	Personal Office	Central block	
9	Question Bank	Central block	
10	Registrar Office	Central block	
11	Server Room	Central block / Block1	
12	UPS/AC	Audi Block	
13	Valuation Center	Block1	
P2 - Medium Priority Departments/Office			
SL.No	**Department**	**Location**	**Resolution duration**
1	Coodinators	Campus	
2	Deans	Campus	
3	Department Printers	Campus	2 Hours
4	HODs	Campus	
5	Lab	Campus	
P3 - Low Priority Departments/Office			
SL.No	**Department**	**Location**	**Resolution duration**
1	Faculty	Campus	
2	Staff	Campus	4 Hours
3	Student	Campus	
P4 - Low Priority Departments/Office			
SL.No	**Department**	**LCD**	**Resolution duration**
1	LCD	Campus	
2	Camera	Campus	8 Hours
3	Wifi	Campus	

Staff and Faculty can register complaints through following Modes

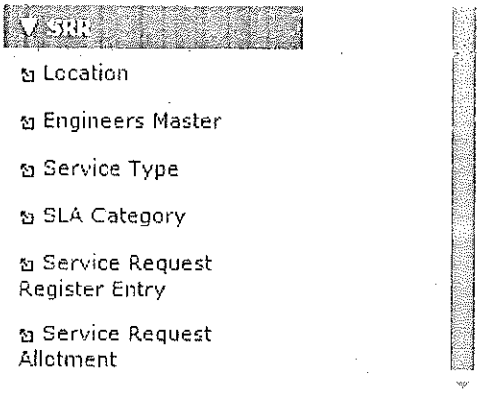
- ERP System
- Mail Service : support@christuniversity.in

- HelpDesk : 9137

Support Requests from faculty, staff and students has been automated by integrating the tracking tool in ERP System. All cases registered by employees through support mail , KP or by helpdesk call will be logged and tracked in this tool Implemented to automate the tracking process to enhance the efficiency of the support system

Call registration and closure intimation is acknowledged to the employee through mail which is auto generated.

Features of the tool

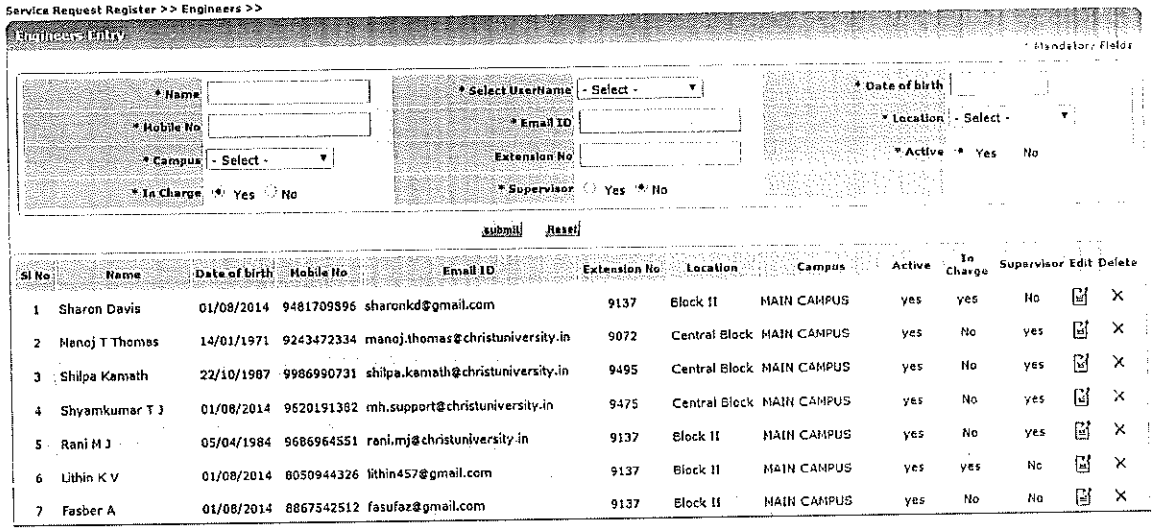


Location: - Engineer's location campus wise

Sl No	Location	Campus	Edit	Delete
1	Block II	MAIN CAMPUS		×
2	Audi Block	MAIN CAMPUS		×
3	Central Block	MAIN CAMPUS		×
4	PU Block	MAIN CAMPUS		×
5	BLOCK I	KENGERI CAMPUS		×
6	BLOCK II	KENGERI CAMPUS		×
7	BLOCK IV	KENGERI CAMPUS		×

Location of engineers in the campus is defined here. Based on the origin of call , calls will be assigned to the location. Engineer will get intimation by mail so that they can check the tool for details and track accordingly. Supervisors will get the mail irrespective of blocks. They can track the calls registered in the campus

Engineers Master


Service Request Register >> Engineers >>

Engineers Entry

* Mandatory Fields

* Name | * Select UserName - Select - | * Date of birth
* Mobile No | * Email ID | * Location - Select -
* Campus - Select - | Extension No | * Active Yes No
* In Charge Yes No | * Supervisor Yes No

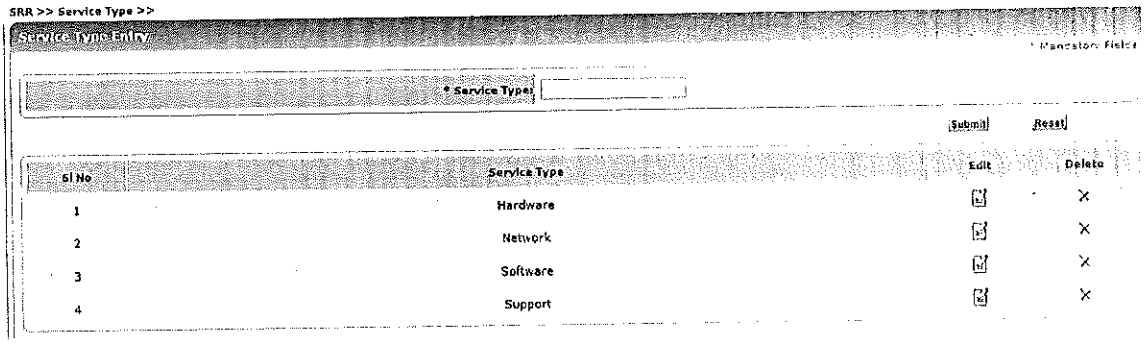
Submit Reset

Sl No	Name	Date of birth	Mobile No	Email ID	Extension No	Location	Campus	Active	In Charge	Supervisor	Edit	Delete
1	Sharon Davis	01/08/2014	9481709896	sharonkd@gmail.com	9137	Block II	MAIN CAMPUS	yes	yes	No		
2	Manoj T Thomas	14/01/1971	9243472334	manoj.thomas@christuniversity.in	9072	Central Block	MAIN CAMPUS	yes	No	yes		
3	Shilpa Kamath	22/10/1987	9986990731	shilpa.kamath@christuniversity.in	9495	Central Block	MAIN CAMPUS	yes	No	yes		
4	Shyamkumar T J	01/08/2014	9620191382	mh.support@christuniversity.in	9475	Central Block	MAIN CAMPUS	yes	No	yes		
5	Rani M J	05/04/1984	9686964551	rani.mj@christuniversity.in	9137	Block II	MAIN CAMPUS	yes	No	yes		
6	Lithin K V	01/08/2014	8050944326	lithin457@gmail.com	9137	Block II	MAIN CAMPUS	yes	yes	No		
7	Fasber A	01/08/2014	8867542512	fasufaz@gmail.com	9137	Block II	MAIN CAMPUS	yes	No	No		

Kengeri

17	Vishnu M P	01/09/2014	8904613170	vishnumpreman007@gmail.com		BLOCK I	KENGERI CAMPUS	yes	yes	No		
18	Shamnas P	01/09/2014	9008430041	pshamnaspalackal@gmail.com		BLOCK II	KENGERI CAMPUS	yes	yes	No		
19	Prasreesh	01/09/2014	8884296800	prasreesh9496@gmail.com		BLOCK IV	KENGERI CAMPUS	yes	yes	No		
20	Vishnu N V	01/09/2014	7795656282	vvisnhupoyil@gmail.com		BLOCK IV	KENGERI CAMPUS	yes	yes	No		

Service Type


SRR >> Service Type >>

Service Type Entry

* Mandatory Fields

* Service Type

Submit Reset

Sl No	Service Type	Edit	Delete
1	Hardware		
2	Network		
3	Software		
4	Support		

To classify the category of support.

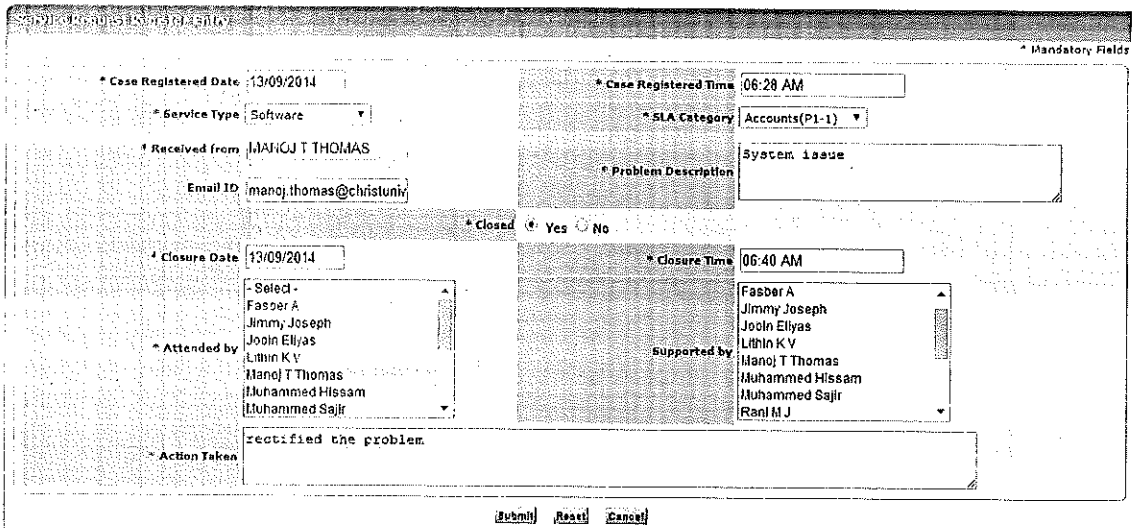
SLA Category

Priority	Campus	Category	SLA	Max. Resolution time in Hrs	Edit	Delete
P1	MAIN CAMPUS	Accounts	yes	1		×
P1	KENGERI CAMPUS	Valuation Center	yes	1		×
P1	KENGERI CAMPUS	Exam Office	yes	1		×
P1	KENGERI CAMPUS	Accounts	yes	1		×
P2	MAIN CAMPUS	Deans	yes	2		×
P2	MAIN CAMPUS	HOD	yes	2		×
P2	MAIN CAMPUS	LAB	yes	2		×
P3	MAIN CAMPUS	Student	yes	4		×
P3	MAIN CAMPUS	Staff	yes	4		×
P3	MAIN CAMPUS	Faculty	yes	4		×

This is to define the resolution time and SLA status. Category is defined with the expected resolution time. If SLA is not met, engineer has to provide the reason for the delay. This can be analyzed in the report

SLA Service Request Register Entry

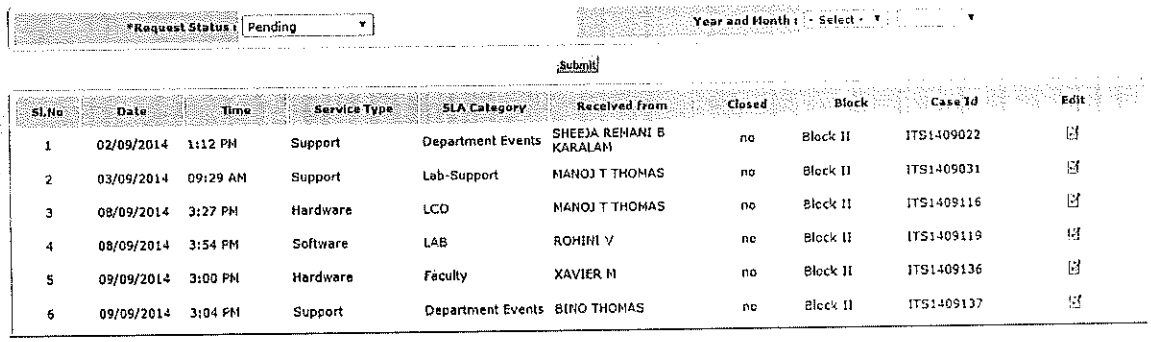
This is available to register call details by engineers.



This screen is available to the engineers to update the call status. All details are updated here to track the efficiency. Problem reported and action taken will be mentioned here. Helpful for analysis and service enhancement

Pending Call status

Engineer View



*Request Status : Pending Year and Month : - Select -

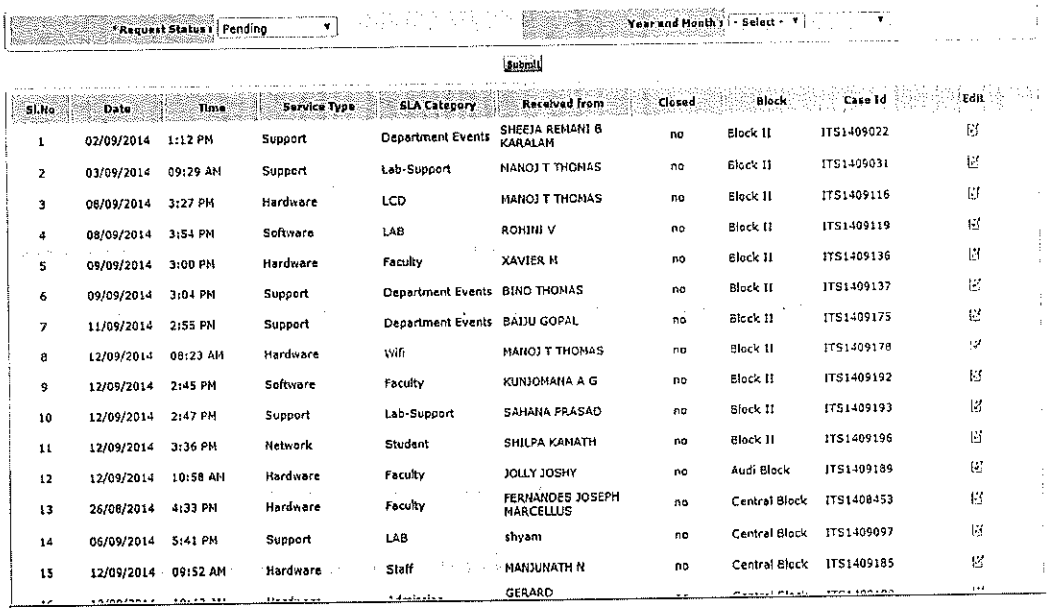
Submit

Sl.No	Date	Time	Service Type	SLA Category	Received from	Closed	Block	Case Id	Edit
1	02/09/2014	1:12 PM	Support	Department Events	SHEEJA REHANI B KARALAM	no	Block II	ITS1409022	
2	03/09/2014	09:29 AM	Support	Lab-Support	MANOJ T THOMAS	no	Block II	ITS1409031	
3	08/09/2014	3:27 PM	Hardware	LCD	MANOJ T THOMAS	no	Block II	ITS1409116	
4	08/09/2014	3:54 PM	Software	LAB	ROHINI V	no	Block II	ITS1409119	
5	09/09/2014	3:00 PM	Hardware	Faculty	XAVIER M	no	Block II	ITS1409136	
6	09/09/2014	3:04 PM	Support	Department Events	BINO THOMAS	no	Block II	ITS1409137	

Engineer can view all calls registered to his location. They can keep track of this to close the call in time.

Block in charges will get an intimation mail whenever call is allocated to his location

Supervisor View



*Request Status : Pending Year and Month : - Select -

Submit

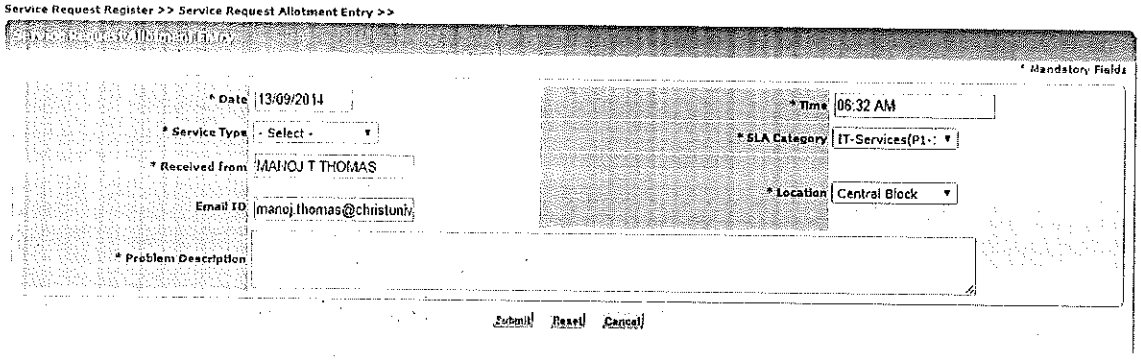
Sl.No	Date	Time	Service Type	SLA Category	Received from	Closed	Block	Case Id	Edit
1	02/09/2014	1:12 PM	Support	Department Events	SHEEJA REHANI B KARALAM	no	Block II	ITS1409022	
2	03/09/2014	09:29 AM	Support	Lab-Support	MANOJ T THOMAS	no	Block II	ITS1409031	
3	08/09/2014	3:27 PM	Hardware	LCD	MANOJ T THOMAS	no	Block II	ITS1409116	
4	08/09/2014	3:54 PM	Software	LAB	ROHINI V	no	Block II	ITS1409119	
5	09/09/2014	3:00 PM	Hardware	Faculty	XAVIER M	no	Block II	ITS1409136	
6	09/09/2014	3:04 PM	Support	Department Events	BINO THOMAS	no	Block II	ITS1409137	
7	11/09/2014	2:55 PM	Support	Department Events	BAIJU GOPAL	no	Block II	ITS1409175	
8	12/09/2014	08:23 AM	Hardware	Wifi	MANOJ T THOMAS	no	Block II	ITS1409178	
9	12/09/2014	2:45 PM	Software	Faculty	KUNJOMANA A G	no	Block II	ITS1409192	
10	12/09/2014	2:47 PM	Support	Lab-Support	SAHANA PRASAD	no	Block II	ITS1409193	
11	12/09/2014	3:36 PM	Network	Student	SHILPA KAMATH	no	Block II	ITS1409196	
12	12/09/2014	10:58 AM	Hardware	Faculty	JOLLY JOSHY	no	Audi Block	ITS1409189	
13	26/08/2014	4:33 PM	Hardware	Faculty	FERNANDES JOSEPH MARCELLUS	no	Central Block	ITS1408453	
14	06/09/2014	5:41 PM	Support	LAB	shyam	no	Central Block	ITS1409097	
15	12/09/2014	09:52 AM	Hardware	Staff	MANJUNATH N	no	Central Block	ITS1409185	
					GERARD				

Supervisors are for the campus. Responsible to track all the calls within the campus. They will get intimation mail whenever call is registered anywhere in the campus. Service call allotment is done by supervisors as below

Service Request allotment

This will be handled by the supervisors. As support request is received by mail, KP or by mail, they can update the details in the tool. Location of the engineers to attend the call will be updated here. Based on which block in charges will get the intimation.

Acknowledgment mail will be sent to the employee requested for the support.



Communication with Registered users

Acknowledgment mail format as below:-

Dear Staff,

Thank you for contacting IT Services!!

Your request is registered with us and has been assigned to the technical team.

Your Request : Cabin No 378, Needs support for the installation of software.

Track ID : ITS1409168

IT Support Team.

Christ University

This is an auto generated mail. Please do not reply. For any queries, contact support@christuniversity.in

After completing the call, engineer will update the call status with closing time and action taken.

Once they complete the entry and submit, closure mail will be sent to the registered employee

Closure Mail format:-

Dear Staff,

Technical team has confirmed that your request has been resolved.

Registered Request : C++ installation in Audi Block lab systems - 45 Nos. Requested by Deepthi Ma'am for 11th september : 11.00 to 1.00 PM Test and be ready by 10th
Track ID : ITS1409105
Action Taken : installed in 50 systems

Regards,

IT Support team

Christ University

This is an auto generated mail. Please do not reply. For any queries, contact support@christuniversity.in

NETWORK SECURITY

Network Security

Network connectivity provided through the University, is governed under the University IT Policy. The Microhard Services Pvt.Ltd is responsible for the ongoing maintenance and support of the Network, exclusive of local applications. Problems within the University's network should be reported to Microhard Services

A.IP Address Allocation

Any computer (PC/Server) that will be connected to the university network, should have an IP address. Following a systematic approach, the range of IP addresses that will be allocated to each faculty/staff/students will be decided. So, any computer connected to the network from the above will be allocated IP address only from that Address pool. Further, each network port in the room from where that computer will be connected will have binding internally with that IP address so that no other person uses that IP address unauthorisedly from any other location. An IP address allocated for a particular computer system should not be used on any other computer even if that other computer belongs to the same individual and will be connected to the same port. IP addresses are given to the computers but not to the ports. IP address for each computer is obtained as per decision of address pool available for various user category

B.DHCP

IP address allocation is handled by DHCP Servers and no manual IP allocation is allowed for any systems.

IT Team system administrator will provide static IP addresses to the servers based on the location of the server which has to be accessed across the campus.Non-compliance to the IP address allocation policy will result in disconnecting the port from which such computer is connected to the network. Connection will be restored after receiving written assurance of compliance from the concerned user.

C. IT Team and departments will be strictly implanting security policy in cooperation with MicroHard Services for the follwoing

1. User Training - Through posters, mails , Training Programs ,IT services shall ensure adequate knowledge exist for appropriate use of assets allocated to users

2. Secure Areas - All important Systems/Servers/Network equipments shall be located in designated Server room. Server room must have access control mechanism or shall kept under lock and a key. Server room access by any personal shall be accompanied by IT-Services personal .

3.Equipment Register - All desktops/laptops/servers are protected with password to protect unauthorized access . UPS Power supBply is provided to all equipments. Critical equipments is placed in placed in places where unauthorized access is minimal.

4. Protection against Malicious code / software - Anti- virus /Anti-Spyware and Anti-Spam software is installed to protect network. Antivirus software is installed at 3 Levels – Gateway at Firewall level, All Servers , Desktops/Laptops.

5. Network Security - Network shall be protected by a Firewall. All equipments must be placed behind the Firewall.All WAN connections are routed through the gateway. Gateway authorizes and authenticate network traffic as per defined access rights on the Firewall

6. Access control - New employees joining the organization shall be provided with userID/MailID as per their roles/responsibilities .Access rights to various servers/application systems. Whenever employee leave the organisation, user ID and Mail account shall be deleted with immediate effect upon receiving informant from HR department. All user ID must have valid password. Password policy can be decided.

7. Security of System Files/utilities - Only authorized users shall be given access to system utilities that allow "Super user" or "Administrative" functions like backup, Network Monitoring etc.

8. Patch Management : IT-Services shall identify operating system and application that require Patch updates. Patch Management plan shall be prepared to

identify the periodicity of monitoring and mechanism for updating all systems shall be recorded.

9. Event logging - Log files of critical servers/equipment (OS) and application systems shall be enabled to track the activities/transaction action performed on the system.

SOFTWARE INSTALLATION LICENSING POLICY AND ASSET MANAGEMENT

Software Installation, Licensing Policy and Asset management

Any computer purchases made by the University should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed. Respecting the anti-piracy laws of the country, University IT policy does not allow any pirated/unauthorized software installation on the university owned computers.

A. Operating System and its Updating

1. Individual users should make sure that respective computer systems have their OS updated in respective of their service packs/patches, through Internet. This is particularly important for all MS Windows based computers (both PCs and Servers). Updating OS by the users helps their computers in fixing bugs and vulnerabilities in the OS that were periodically detected by the Microsoft for which it provides patches/service packs to fix them. Checking for updates and updating of the OS should be performed at least once in a week or so.

2. University as a policy encourages user community to go for open source software such as Linux, Open office to be used on their systems wherever possible.

3. Any MS Windows OS based computer that is connected to the network should be updated with all the patches. Microhard Services is responsible for keeping all machines up to date by regular preventive maintenance activities

B. Antivirus Software and its updating

1. Computer systems used in the university should have anti-virus software installed, and it should be active at all times. The primary user of a computer system is responsible for keeping the computer system compliant with this virus protection policy.

2. Individual users should make sure that respective computer systems have current virus protection software installed and maintained. He/she should make sure that the software is running correctly. It may be noted that any antivirus software that is running on a computer, which is not updated or not renewed after its warranty period, is of practically no use. If these responsibilities appear beyond the end user's

technical skills, the end-user is responsible for seeking assistance from Microhard Services.

IT Admin team will disconnect all user devices from the network if found without active Antivirus software

Software Asset Management

Asset Register is maintained by IT admin team . All the Purchase is done as per the IT purchase policy and Asset register is maintained for the same. Softwares purchased by the department shall maintain software in their department in consultation with IT department. Asset register and renewal of the license is the responsibility of IT Department. Asset register must include the department using the software , License type, validity and vendor contact details.

IT SERVICES ACCOUNT USAGE POLICY

IT Services Account Usage Policy

Any user (student / staff) is provided with login credentials to access Email , ERP account, Internet access account and Library account . IT department provide login credential to all students join the university. This is based on the student list provided by the admission office. Account credentials for the staff is provided by the IT department based on the confirmation by the personal relations department.

Email Account : Email service is provided by gmail all the staff and students will be provided personal email ID upon joining the university. Email format will be firstname.lastname@christuniversity.in for staff and fisrtname.lastname@course.christunivesrity.in for students. Email will be available for students as long as they are studying in the university and will be inactivated one they leave the institute. Staff email account will be inactivated once they leave the institution and will be active only for 15 days.

EPR Account/Internet account/library Account will inactivated with immediate effect once the student/ staff leave the University

INFORMATION SECURITY

Information Security

Information is security management is the combined responsibility of IT Department and Micro hard Services.

IT Department training division emphasize on information security policy during training sessions and guide lines given for all desktop users in the university

Information security recommendations include:

1. All desktop computers should have the latest version of antivirus and should retain the setting that schedules regular updates of virus definitions from the central server. Kasperskey Antivirus is deployed in the campus . Maintenance of Antivirus with latest patch is the responsibility of the Microhard Services.

2. When a desktop computer is installed, all operating system updates and patches should be applied. In addition, operating system updates and patches should be applied regularly, on an ongoing basis.

3. All Windows desktops (and OS X or later Macintosh desktops) should have an administrator account that is not used as the regular login account. The login for the administrator account should be changed from the default. Administrator login details are known only the IT Department and Microhard Services

4. The password should be difficult to break. Password, defined as: i. must be minimum of 6-8 characters in length ii. must include alphanumeric characters. Do not leave password blank and x. Make it a point to change default passwords given by the software at the time of installation

5. The password for the user login should follow the same parameters as mentioned above.

6. The guest account should be disabled.

7. New machines should activate the built-in firewall.

8. All users should consider use of a personal firewall that generally comes along the anti-virus software, if the OS does not have an in-built firewall.

9. All the software on the compromised computer systems should be re-installed from scratch (i.e. erase the hard drive and start fresh from installation disks). When the hard disk of the PC is formatted, the OS and all the application software should be installed from the original CDs of the software. Only the data or document files should be copied from the old hard disk and care should be taken to see that no virus residing in the old hard disk gets into the newly formatted and installed hard disk.

10. All Servers password policy is same as point No.4 and is known only to the IT Department. Access to the server room is restricted and is only allowed only with some one in the IT Department

IT RISK MANAGEMENT

IT Risk Management

Disaster recovery management is very crucial for the university. All the servers and services offered by the IT departments is maintained and managed by the University. IT team is responsible to implement and maintain all the servers hosting the services. High availability and disaster recovery is the responsibility of IT Department.

High Availability: Unavailability of Services like ERP, LMS , Gmail , Internet access has to be considered seriously as it affects the day to day activities of students and staff in the campus. Server implementation architecture is focused to handle such scenario. Load balancing and replication strategies are implemented to address such issues along with performance gain. Daily check by the IT team and documentation of down time on the same is to analyze and improve the high availability factor.

Disaster recovery: Backup and recovery plan is defined by the IT Department to effectively manage the risk with the down time of services. ERP system / LMS systems and all other servers is scheduled with daily back. NAS backup device is implemented and backup is automated daily. Replication architecture is implemented for Database servers to avoid the risk of losing the data. Critical application servers are maintained in separate locations to avoid gods act like Fire, Flood etc. Server rooms is different locations and synchronization of data across the locations is effective for high availability

OPEN SOURCE RESOURCES

Open Source resources

Christ University is strictly following the policy of Open Source resources for all the services provide to users and staff. All servers are hosted and maintained by the University. Campus ERP system (KP) / Learning Management system(Moodle), Library applications are all implemented on Linux System.

We promote the use of open source resources as they are secure, fast and scalable

Green Computing

University is environmentally responsible and is for eco-friendly use of **computers** and their resources. We use and dispose computing devices in a way that reduces their environmental impact.

A. Conserve Energy :

Desktop systems and servers are always set with power saving mode. Microhard services is responsible for implementing in all systems which are installed. Regular check is done by Microhard Services to make sure that power consumption mode is enabled affectivity

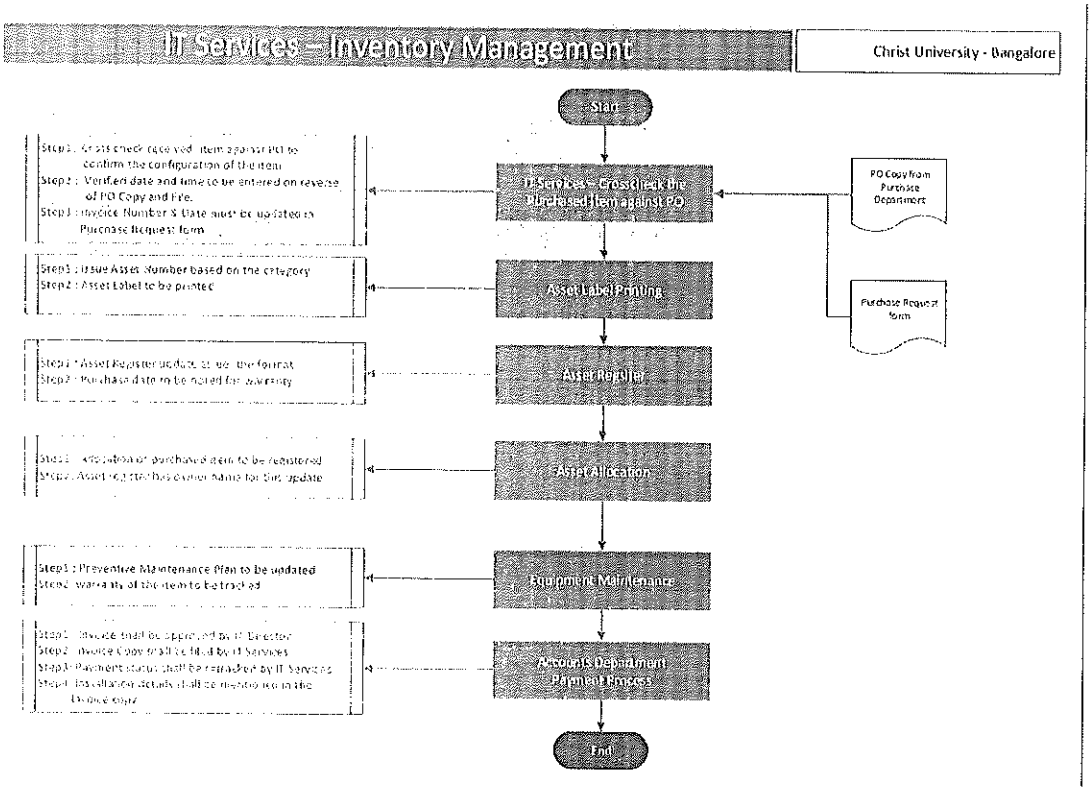
B. Reduce paper consumption:

MailID is provided to all staff members and students so they can effectively communicate using soft copies. WIFI is enabled through out the campus to ensure the communication using devices. Departments are provided with common network printer with dual side printing facility. Training is provided by IT team to avoid paper wastage by single side printing

C. Recycle :

University discards the used or unwanted electronic equipment is a responsible manner. Microhard services is responsible to maintain all the hardware equipments within the campus. University has a contract with Microhard service to take back all the obsolete equipments from the campus premises and is the responsibility of Microhard Services to discard it wisely. University will not discard used devices within the campus premises

IT Inventory Management



IT Purchase process