



AISSMS

INSTITUTE OF INFORMATION TECHNOLOGY

(IOIT)



ADDING VALUE TO ENGINEERING

An Autonomous Institute Affiliated to Savitribai Phule Pune University
Approved by AICTE, New Delhi and Recognised by Govt. of Maharashtra
Accredited by NAAC with "A+" Grade | NBA - 5 UG Programmes

Network and Internet

Institution's IT policy

Developed

By

Network and Internet Committee

AISSMS IOIT, Pune



Handwritten signature in blue ink.

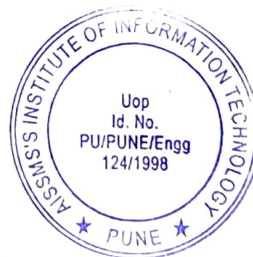
Principal
AISSMSIOIT, PUNE

Contents

- 1. Introduction**
- 2. Objectives**
- 3. Why IT Policy**
- 4. IT Policy**
- 5. Network (Intranet & Internet) Use Policy**
 - a) IP Address Allocation**
 - b) DHCP**
 - c) Running Network Services on Firewall**
 - d) Wireless Local Area Networks**
- 6. Guidelines for Departments Running Application or Servers**
- 7. Web Application Filter**
- 8. Beneficiaries**
- 9. Resources**

✓

Principal
AISSMSIOIT, PUNE



1. Introduction

Due to the technology evolutions, it is the necessity to look at all possible information technologies comprehensively for quality enhancement in teaching learning at The All India Shri Shivaji Memorial Society's Institute of Information Technology, Pune. The widespread selection of IT for the development of education holistically could be realized based on strong IT policy. The plan to build an IT Policy of the institute is motivated by the immense capability of IT for increasing reachability and advancing quality of education. The built policy undertakes to provide guidelines to facilitates the stakeholders of AISSMS IOIT in optimizing the usage of IT resources. Belonging users are adhering to all the mentioned policies at present.

2. Objectives

- To develop, support and withstand IT and activities which are IT enabled and ensure improved access, quality and throughput in the education system of the Institute.
- To innovatively participate in the organization, provisions and expansion towards all-round socio-economic development of the nation and global competence.

3. Why IT Policy

- By keeping in mind the fair and transparent academic process IT Policy is being documented towards the use of IT resources in the Institute for all stakeholders such as Faculties, Students, Guests and Research Scholars.
- Because of the provisioning of policy and academic activities, IT resource utilization in the Institute has grown during the last decade.

Now, AISSMS IOIT has network and internet connections to each computer machine covering the entire building of the institute.

Network and Internet Committee is the cell that has been given the responsibility of running the institute's network and Internet facilities.

Network and Internet Committee is running the SOPHOSH Hardware Firewall security, DHCP, DNS, email, web and application servers and handling the network of the institute.


Principal
AISSMSIOIT, PUNE



AISSMS IOIT is availing the Internet bandwidth from CloudInsta 24 Services Pvt. Ltd.(Channel Partner Tata Communication Limited). Total bandwidth availability from CloudInsta24-TCL service provider is 450 Mbps (leased line 1:1).

Due to exhaustive usage of the Internet, the performance of network degrades in following three major ways:

- Internet traffic over the Wide Area Network (WAN) is a significant bottleneck as compare to high speed of Local Area Network (LAN).
- If users are given full accessibility of Internet, downloads may cause congestion in traffic, which result in poor Quality of Service (QoS), due to which critical users and applications may be affected badly.
- The time when all computer machines are connected in network, rapid spread of viruses that entered into LAN, through Intranet/internet, among other computer machines on the network, which increase the possibilities of exploitation of vulnerabilities of the OS.

Large number of simultaneous users over highspeed LANs try to consume Internet resources through a limited bandwidth, will disturb bandwidth availability.

Viruses corrupt files, spread quickly and when these infected files are sent to other PCs over internet are difficult to exterminate. Few viruses damage the files as well as static storages, resulting loss to the institution. Some viruses obtain network space and slow down the network by replicating infected files.


Principal
AISSMSIOIT, PUNE



4. IT Policy

The IT Policy of the AISSMS IOIT is comprising of the following.


IT Ethics / Ethics Policy

- **Persistence**

The All India Shri Shivaji Memorial Society's Institute of Information Technology, Pune, always encourages incessant learning, experiential learning and the skill development of adult learners. The Institute is devoted to admire privacy of users and expects that each user to act in a liable, legal, ethical and efficient way whenever using IT facilities and resources of the Institute.

- **Policy Statement**

The All India Shri Shivaji Memorial Society's Institute of Information Technology, Pune provides access to IT resources for faculty, staff, students, and guests to support the mission of the Institute. Each legitimate and authenticated user of IT resources at Institute is accountable for ethical, efficient and legal utilization of these resources.


Principal
AISSMS IOIT PUNE



5. Network (Intranet & Internet) Use Policy

Network connectivity provided through authenticated network access connection or Wi-Fi is under the institute IT Policy. The Network and Internet Committee is responsible for the on the spot maintenance and support of the Network. Problems within the institute's network should be reported to Network and Internet Committee.

a) IP Address Allocation

Any computer (PC/Device) that will be connected to the institute network should have an IP address assigned by the System Department. Departments should follow a systematic approach, the range of IP addresses that will be allocated to each PC/Device in the building as decided. So, any PC/device connected to the network from that building will be allocated IP address only from that Address pool. IP allocation and its usage is exclusive for the AISSMS IOIT premise only and no external entity can use the IP pool from other location.

At the time when new PC/Device is installed in the building, IP address allocation is done dynamically from firewall installed by Network and Internet Committee. There is a provision made to avoid IP conflict.

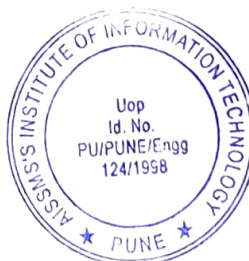
b) DHCP

Class-B of network is used to create possibility of connecting more number of concurrent PC/Devices in the network. All these activities are configured on SOPHOSH XGS-2300 Hardware firewall. SOPHOSH XGS-2300 Hardware firewall and all PCs/Devices are connected through switches/hubs/routers/access points installed on various locations in the premises. Applications/Softwares/Operating System which are configuring their own DHCP server is strictly be avoided, as it is considered absolute violation of IP address allocation policy of the institute. In the same line, configuration of proxy servers is also be prohibited to avoid interference with the service run by Network and Internet Committee.

c) Running Network Services on Firewall

With the concern of Network and Internet Committee only users of AISSMS IOIT can run server version of software such as HTTP, SMTP, FTP servers etc by giving proper justification of the requirement and approval of principal. Ignorance on this policy is a direct violation of the institute IT policy, and will result in disconnection from the Network.

Principal
AISSMSIOIT, PUNE



Network and Internet Committee is not responsible for the content of PCs/Devices connected to the Network regardless of its being Institute or personal property. Network and Internet Committee will be forced to disconnect clients where potentially damaging software is found.

A client may also be disconnected if the client's activity negatively impacts the Network's performance.

Traffic on the Network will be continuously monitored for security and for performance by Network and Internet Committee.

Captive Portal

The administrator configures users' personal details, such as name, sign-in credentials, email address, and user-group membership, when they're registered. The user group applies a set of policies that define the group members' surfing quota, access time quota, and network traffic quota. The surfing quota policy defines the user account expiry date, while the access time policy defines the total number of allowed internet usage hours. The data transfer policy defines upload and download data transfer restrictions.

The administrator and user can view the user details. The administrator can view the details of a user in the device, while a user can view them on the user portal.

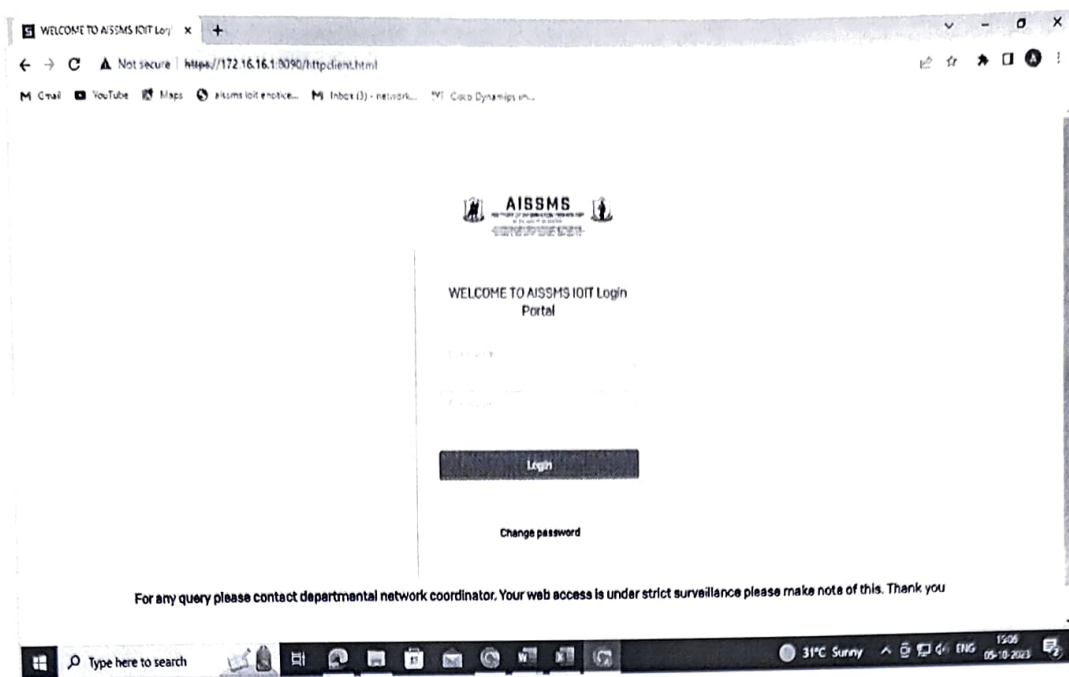
Access the user portal

You can access the user portal in the following ways:

- Browse to <https://172.16.16.1:8090>.
- Go to the captive portal and Sign in to the portal using your user's sign-in credentials.


Principal
AISSMSIIT, PUNE





For the access of Internet facility in the AISSMS IOIT premises each user has to login on the configured Captive portal on hardware firewall. Auto Log off policy is applied to each user in the following cases:

- Captive portal screen is closed by user.
- PC turned off by mistake or due to power failure.
- If PC on which the Captive portal login is done has gone in Idle stage.
- If Parallel login limit is crossed(Never observed yet)
- In case of wireless devices, if Wi-Fi router is going out range or change of Wi-Fi router.
- In case of Wired LAN if the associated switch got turned off somehow or reset.

In case of update with new firmware patches on SOPHOSH Firewall, Update of Firmware on firewall is mostly done in night somewhere around 10:30pm manually to avoid the inconvenience may be faced by the live users during working hours.

d) Wireless Local Area Networks

This policy applies, in each department wireless local area networks. In addition to the requirements of this policy, departments must get their respective wireless routers/access points configured from Network and Internet Committee. Departments or individuals should not configure Wi-Fi with unrestricted access.

Principal
AISSMS IOIT, PUNE



6. Guidelines for Departments Running Application or Servers

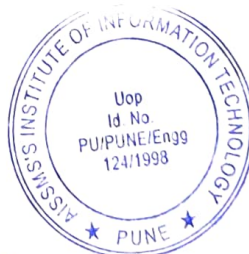
Respective departments may run applications or various servers for practical or skill development courses. They are responsible for maintaining their own servers.

- Firstly obtain an IP address from Network and Internet Committee to be used on the server.
- Acquire the hostname of the server entered in the DNS server for IP Address resolution.
- Ensure that only the services that are essential for running the server for the purpose it is intended for should be enabled on the server.
- Ensure that the server is protected adequately against virus attacks and intrusions, by installing the appropriate software such as anti-virus, intrusion prevention, personal firewall, anti -spam etc.
- Operating System and the other security software should be periodically updated.

7. Web Application Filter

Application	Management	Staff	Student	Guest
Captive portal session	3/1 concurrent sessions/user			
Sites Blocked	Porn, torrents, Proxy & Hacking, Gambling, Criminal Activity			
YouTube	Allow	Allow	Allow	Allow
YouTube Educational	Mandatory Certification needs to be purchased			
What's App	Allow	Allow	Deny	Allow
Facebook	Allow	Allow	Deny	Allow
Skype or Video Calling	Allow	Allow	Deny	Allow
Entertainment	Allow	Deny	Deny	Allow
TV News Channel	Allow	Allow	Allow	Allow
Online Games	Deny	Deny	Deny	Deny
Windows Update	Allow	Allow	Allow	Allow


Principal
AISSMSIOIT, PUNE



Default Block Category In Firewall

- Criminal Activities
- Hunting & Phishing
- Malware & Ransomware
- Culture and Entertainment
- Extreme or Violent Web Content
- Games and Gambling
- Nudity and Adult Content
- Online Shopping
- Risky Downloads
- Suspicious

Default Allowed Category in Firewall

- Government
- University
- Education

8. Beneficiaries

In campus Stakeholders of All India Shri Shivaji Memorial Society's Institute of Information Technology, Pune. These users are solely responsible for reading, understanding, and complying with this policy.

- Students: UG, PG, Research
- Faculty Members
- Administrative Staff (Non-Technical / Technical)
- Higher Authorities and Officers
- Guests


Principal
AISSMSIOIT, PUNE



9. Resources

- SOPHOSH XGS-2300 Hardware Firewall
- Network Devices wired/ wireless
- Internet Access
- Desktop / Mobile/ Server


Principal
AISSMSIOIT, PUNE

