IT Policy

for

SIES

This Internal document has been made to implement IT policies & guidelines that are relevant in the context of SIES. While creating these policies, every effort has been made to have a careful balance between security and the ability to conduct the rightful activity by the users. Due to the dynamic nature of the Information Technology discipline, Information security in general and therefore policies that govern information security process are also dynamic in nature. IT Policies mentioned herein need to be reviewed on a regular basis and modified to reflect changing technology, changing requirements of the IT user community, and operating procedures and identified threats. Purpose of IT policy is to set direction and provide information about acceptable actions and prohibited actions or policy violations. Guidelines provided will help organisation, departments and individuals who are part of SIES community to understand how SIES policy applies to some of the significant areas and to bring conformance with stated policies.

Version Control History:

Version	Prepared by	Date	Reviewed by	Date
Draft V.0	Mr. Pankaj Srivastava	Jan, 2020	Mr. MV Ramnarayan	Feb, 2020

Index

Contents

1. Preamble - Need for IT Policy

In today's digital era, IT services are among the most critical functions in any educational institution & research organization. IT has the responsibility to avoid inappropriate or illegal internet or software use that creates risks for our organization's legality and reputation.

Over the last 15 years, not only active users of the network facilities have increased many folds but also the web-based applications have increased. IT is managing the Firewall security, Proxy, DHCP, DNS, email, web application servers including the complete network of the SIES. SIES is getting its Internet bandwidth from ISP's. When users are given free access to the Internet, non-critical downloads may clog the traffic, resulting in poor Quality of Service (QoS) and affecting critical users and applications. Too many concurrent users who are on the high speed LANs trying to access Internet resources through a limited bandwidth, definitely create stress on the Internet bandwidth available. Hence, balancing the internet bandwidth per user is the key to effective internet management.

Computer viruses attach themselves to files, spread quickly when files are sent to others and are difficult to eradicate. Some can damage the files as well as reformat the hard drive, causing extensive loss to the enterprise. They can slow down or even bring the network to a halt. Staff is easily prone to Malwares through infectious links sent via email which can cause encryption and lock down the IT equipment's and demand ransomware. Time and resource is lost with a workstation being scanned and cleaned of the virus and back up. So preventing Virus, Malwares, etc. from attacking the campus IT network is crucial and IT has to take steps in order to secure the network by installing firewalls and monitoring logs through automated tools, having access control mechanisms and use of AI to optimise prevention of virus intrusion and content filtering software at the perimeter gateway.

However, in the absence of clearly defined IT policies, it is extremely difficult to convince users about the steps that are taken for managing the network. Users tend to feel that such restrictions are unwarranted, unjustified and infringing the freedom of users. As IT users are aware, all the educational institutions worldwide have IT policies implemented in their respective institutions. Without strong management policies, IT security measures will not be effective and not necessarily align with management objectives and desires. Hence, policies and guidelines form the foundation of the Institution's security program. Effective policies are a sign of due diligence; often necessary in the event of an IT audit or litigation. Hence, a formal IT policy needs to exist to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by SIES on the campus. IT usage policies outline our guidelines for using internet connection, Network and all the IT equipment's in campus.

This policy establishes strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the SIES. Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information (via VOIP) within the campus network. Policies also serve as blueprints that help the institution implement security measures. An effective security policy is as necessary to a good information security program as a solid foundation to the building.

Hence, SIES also is proposing to have its own IT Policy that works as guidelines for using the SIES's computing facilities including computer hardware, software, email, information resources, Network - intranet and Internet access facilities, collectively called "**IT POLICY**".

2. Scope of IT policy & Classification

IT Policy will be applicable to below identified groups accessing IT network services and all the electronic IT equipment like desktops, laptops, iPad, mobile, USB drives, printers, scanners, servers etc.:

1. End Users Groups (Trustee, Admin Staff, Faculty, Students).
2. IT System and Network Administrators.
3. Third party Partners/Resources operating onsite using the IT Infra Network of the SIES.
4. External visiting Guests, Alumni

IT policies is classified into following groups:

1. General Computer Facilities usage policy.
2. Device & Peripheral (Desktop/Laptop/Tablet) usage policy.
3. Email Usage Policy.
4. Software Installation and Licensing Policy.
5. Network Use Policy.
6. Password Policy
7. Social Media Policy

This IT policy also applies to the IT resources administered by the central IT team and is applicable to all institutes under SIES across India. Areas will include administrative departments such as Classrooms, common passage, usage and utility areas in the Institute building, Conference Rooms, Library, Computer Centres, Laboratories, or Hostels and Guest houses, or Residences wherever the IT network facility is provided by the SIES.

Computers owned by the individuals, or those owned by research projects of the faculty, when connected to campus network are subjected to the Do's and Don'ts detailed in the SIES BYOD - IT policy.

Further, all the faculty, students, staff, departments, authorised visitors/visiting faculty and others who may be granted permission to use the SIES's information technology infrastructure, must comply with the Guidelines. Certain violations of IT policy laid down by the SIES by any SIES member may even result in disciplinary action against the offender by the SIES authorities. If the matter involves illegal action, law enforcement agencies may become involved for appropriate action and SIES will not be responsible for individual's actions.

3. General Computer Facilities Usage Policy

Our organization permits Members reasonable personal use of computing facilities. You should be careful not to misuse these facilities, for instance by:

1. Causing wilful damage
2. Removing equipment - The Organization provides facilities for the benefit of all members, removing equipment means others cannot use it for work or study
3. Hacking – attempting to access systems or information within or outside the Organization without authority, or encouraging others to do so
4. Using the Internet in a way which is contrary to the various statements listed in this document. Rules laid down by the Organization.
5. Sending communications (email, etc.) which constitute bullying or harassment or bullying.
6. Causing unintended high volumes of traffic on the internet.
7. Impersonation of others, e.g. sending an email which does not appear to come from you
8. You should use official email id only; for all the official communication. Personal email id like Gmail, Hotmail etc. must be avoided for office work.
9. You must preserve all the emails received & sent by you for official purposes.
10. Emails are considered to be vital evidence in the court of law & hence the requirement.
11. You are obliged to follow all the laws of the land pertaining to usage of IT.

Use of the Organization IT Resources including the IT Network for any illegal, defamatory, indecent purpose is prohibited and punishable as per applicable Indian IT act/law.

4. Device (Desktop/Laptop/Tablet) Usage policy

These guidelines are meant for all staff using the SIES provided 'devices' (Desktops, Laptops, Tablet, etc).

1. Devices will have the latest version of antivirus and retain the setting that schedules regular updates of virus definitions from the central server.
2. When a new desktop is provisioned on network, all latest operating system updates and patches will be applied. In addition, operating system updates and patches should be applied regularly, on an ongoing basis either remotely or manually as per security policies set at the server level and applied to the desktop machines.
3. All Windows desktops and MAC's should have an administrator account that is not used as the regular login account.
4. The guest account will be disabled by default.
5. End users should regularly backup their files to file server.
6. If any PC is compromised, IT will isolate the PC / shut down the LAN port.

5. Email Usage Policy

Email accounts are automatically assigned to Organization members. Members may make reasonable personal use of computing facilities provided as long as this does not interfere with the functioning of the organization network or cause any difficulty or distress to others.

Because electronic communications can sometimes go astray, highly confidential or sensitive information should not be transmitted via e-mail unless it is encrypted.

When composing and sending emails, the following guidelines should be observed:

- Always display courtesy when writing and sending messages
- Emails can be produced in a Court of Law, so consider if the content is appropriate before sending one.
- Defamatory statements should never be written in email messages
- Users should ensure that their password & login ids are not shared with others. The users will be responsible for any communication taking place through their IDs. It is preferable that your passwords are changed periodically. In case you suspect that your password/ ids are compromised, inform IT helpdesk for help.

6. Software Installation and Licensing Policy

User should not install/ uninstall software on any computer owned by the Organization, or reconfigure one without the approval of the IT Department concerned authorities. Any additional software if required, you will raise a request through your HOD to IT. It is essential for the official purpose, it may be approved by respective department head and IT head. Only after prior approval of the IT in-charge of the organization or unit, that the new software can be downloaded.

All installed software must be correctly licenced for use. The use of counterfeit software as well as illegal software's will put your personal/ official data at risk as many products will have been pre-seeded with Malware.

Users may not make use of the Organization's IT facilities for private financial gain or for commercial purposes outside the scope of official duties or functions, without specific authorisation to do so.

7. Network use policy

It is illegal to download, use or re-distribute unlicensed copies of copyright material, such as music, films, or computer software codes/programs. If you do this, you will be personally liable for prosecution. The Organization is also liable for prosecution if they allow their networks or computers to be used in this way. For that reason, such activities are strictly prohibited.

The below Network Rules will be in force.

1. The name of the Organization shall not be brought into disrepute.

2. High-bandwidth applications (such as streaming audio, streaming video, internet phone/video conferencing) must only be used sparingly, as they increase network traffic. Individuals who generate high levels of traffic may be tracked and contacted;

3. It is forbidden to download, use or re-distribute copies of copyright material unless the user is in possession of a valid licence to do so.

4. It is forbidden to run any 'peer-to-peer' or 'file-sharing' software. As well as being the main route for illegally downloading and re-distributing copyright material, these programs can generate large quantities of chargeable internet traffic and can adversely affect the performance of our network. Microsoft Team's as a collaboration tool and OneDrive for File sharing may be used.

5. You must not send emails or create posts which appear to come from somebody else or from a fictitious address.

6. You must only use the IP number(s) issued by the Institution or organization. No 'spoofing', or attempts to use other IP numbers, is permitted.

7. Routing/ Switching/ Wireless equipment's must not be connected to the network. Ethernet hubs and switches may be used with prior approval from the IT Department.

8. These can present a security risk and can interfere with the Organization's network and wireless coverage.

9. In particular, these regulations forbid the use of the network for any illegal, defamatory, or indecent purpose.

10. Promiscuous mode reception or any other form of network traffic monitoring is forbidden.

11. User machines are forbidden to saturate the network by emitting an unreasonably high frequency of packets, or to attempt any other form of denial of service to others.

12. Sending email from @SIES account using a client (such as Outlook) may only be done via official SMTP mail servers in the SIES domain.

13. Inward e-mail to private SMTP servers is not permitted.

14. IP packet forwarding is forbidden (note that you might have to explicitly turn off IP forwarding with some versions of Linux).

15. Where a user machine offers an allowed service to the network, the service must comply with relevant acceptable use policies. For instance, if a Telnet service is offered, it must not offer resources outside the SIES domain unless the usage complies with the IT Usage Acceptable and Information Technology Syndicate rules.

16. No person can create a new domain or server etc. within our network.

17. SIES reserves right to perform necessary audits from time to time to check if any unauthorized/ illegal activities are being done by anyone. If found guilty, necessary actions will be initiated against the person.

8. Strong Password Policy

1. The login for the administrator account will be restricted to certain users only and will be changed on periodic basis.
2. The passwords should follow the same parameters outlined below.
    a. Must be minimum of 6-8 characters in length
    b. Must include punctuation such as ! $ % & * , . ? + - = iii.
    c. Must start and end with letters
    d. Must not include the characters # @ ' " `
    e. Must be new, not used before
    f. Avoid using your own name, or names of your wife or children, or name of your department, or room No. or house No. etc.
    g. Passwords should be changed periodically and also when suspected that it is known to others.
    h. Never use 'NOPASS' as your password
    i. Do not leave password blank
3. Make it a point to change default passwords given by the software at the time of installation.

9. Social Media Policy

Some members of the organization are allowed the social media access. The Organization recognises that Members use social media such as Whatsup, Facebook, Twitter, LinkedIn and blogs to talk about their lives and interests, and it supports the responsible use of this technology.

The following guidance has been developed in the use of social media:

1. You should be careful with what you post online. Most sites are public by default and others may see what you post. You will not be able to control who sees it as information can be forwarded, you are responsible for what you post. Once you post something it becomes a permanent record in the eyes of the law
2. Comments either in an official or personal capacity which could be regarded as abusive, humiliating, discriminatory, derogatory or could adversely affect a member's life in Organization will be treated as a serious disciplinary offence
3. The Organization's Respect and Dignity Policy should be observed when using social media to make posts.

10. Penalties

The penalties for breaking these rules include fines and/or permanent disconnection of facility for the individual without any refund and further will depend on the severity of the breach, the legal actions will be taken by management.

The IT Department hopes to resolve any rule infringements through contact with the person involved before taking any direct action. We, however, reserve the right to disconnect without warning if we receive notification that your machine has downloaded or uploaded copyright material, if you are found to be generating unreasonably large amounts of internet traffic, or if your machine appears to be causing a network problem or you have downloaded any illegal software.

Any person who misuses IT facilities or who uses IT facilities for private financial gain or for commercial purposes, with or without specific authorization to do so, may be charged with the cost of such use or misuse at a rate determined from time to time by the appropriate Authorized person from the organization. If any person who has been so charged with the cost of IT resources fails to make reimbursement, any authorization to use IT facilities shall be suspended automatically until reimbursement is made in full, and the matter shall be reported by the Central team to the appropriate Organization or Organization financial authority.