SYMBIOSIS

Symbiosis Information Technology Policy 2014

Table of Contents

1. IT Policy and Governance

This policy manual is a compilation of the Information Technology policies and procedures of Symbiosis approved by **the Managing Committee of Symbiosis Society and the Board of Management of SIU** from time to time. This Information Technology policy termed as "IT Policy" supersedes the IT policies issued earlier if any.

IT Policies are formulated for planning, procuring, setting up, administering, maintaining, updating and scrapping of IT Resources. The word 'Symbiosis' used in IT Policies, includes Symbiosis Society and Symbiosis International University and all the institutes, departments and entities under them.

Symbiosis believes that appropriate IT systems are essential for delivering quality academics, efficient administration and transparent communication. A comprehensive IT policy is therefore formulated to maintain quality of service and smooth functioning of secure systems in achieving the vision and mission of Symbiosis.

1.1 Applicability of IT Policy

This Policy applies to everyone who accesses Symbiosis Information Technology Resources, whether a part of Symbiosis or not, whether on campus or from remote locations, including but not limited to students, teaching staff, non-teaching staff, technical staff, vendors, consultants, guests, volunteers or any other persons associated with Symbiosis and who are allowed to use Symbiosis IT resources. . By accessing Symbiosis Information Technology Resources, the user of the resources agrees to comply with this Policy.

1.2 Background

1. Symbiosis started building its IT infrastructure at its autonomous institutes mainly for teaching of technology and computerizing manual document keeping. As the technology advanced, the individual institutes kept up with the changing technology and brought in improved IT systems in academics and in administration. Subsequently, the departments of Symbiosis Society and Symbiosis International University made a

major progress in streamlining of various functional systems such as Finance and Examination, encompassing all institutes under its functional reach to bring in more efficiency, integration and consolidation. IT today has become an essential and integral part of the academic and administrative processes at Symbiosis as it has grown into a large family consisting of Symbiosis International University, its constituent institutes, Grant-in-aid College, health centres, schools and museums.

2. At Symbiosis, the IT systems were built independently at an initiative of individual institutes or departments. With a phenomenal growth of Symbiosis, there have been multiple IT application systems for similar functions although computer hardware has remained relatively uniform. It has therefore become necessary to establish a common IT governance model for all institutes and departments under the umbrella of Symbiosis Society.

3. This IT Policy framework is the first step towards bringing uniformity in the IT infrastructure across Symbiosis. The purpose of this document is to clearly indicate the appropriate and approved activities and notify prohibited actions which can constitute policy violations. Policy guidelines will help various institutes, departments and individuals to ascertain the rightful use of the IT resources and facilities, the ownership of which rests with Symbiosis Society.

4. These policies draw from the principles, guidelines, and norms established by recognised international bodies and standards such as ISO 27001 (BS7799), IEEE, CoBit and ITIL.

1.3 Primary Goals

The IT policy of Symbiosis aims at introducing the principle of IT Governance across Symbiosis for achieving uniformity in the management of IT infrastructure, safeguarding all IT resources, laying down guidelines for ensuring continuous improvement in the performance, operations and maintenance of all IT services. It also includes best practices for administering IT resources and facilities, and authorization of accesses to the users.

1.4 Stakeholders

1. The main stakeholders are
    a. Symbiosis Society (SS)
    b. Symbiosis International University (SIU)
    c. Departments of Symbiosis Society
    d. Departments of Symbiosis International University or any other entity directly under SIU
    e. The constituent institutes of Symbiosis International University
    f. Grant-in-aid colleges under Symbiosis Society
    g. Schools under Symbiosis Society
    h. Museums under Symbiosis Society
    i. Any other entity which uses IT resources of Symbiosis Society.

    In this document the word "Institute" represents all the above entities except SS & SIU.
2. The other important stakeholders are the users of IT resources viz.
    a. Students
    b. Employees (Faculty and Staff who are full time or part time)
    c. Visiting Faculty
    d. Authorised vendors
    e. Authorised Visitors and Guests.

    In this document the word "User" represents all the above entities which carry out any transaction in the IT systems of Symbiosis.

1.5 IT Resources

The IT Resources of Symbiosis include the following:

a. Computing Hardware Systems including peripherals and storage,
b. Networking Devices including firewall systems
c. Display devices (e.g. projectors, intelligent display boards etc…)
d. Systems Software such as Operating Systems, Database Systems, Networking Systems, Anti-virus software and any other software that facilitates an application to function on computing hardware
e. Application Software and firmware
f. Communication devices and Software including Videoconferencing, Email etc.
g. Web sites (blogs, FB pages, Twitter handle and other online resources)
h. Subscribed IT services such as global databases (e.g. EBSCO, etc..)
i. Any other resource using IT

In this document the word "IT System" represents one or more of the above resources connected together to perform a function.

IT Resources that are not of consumable nature are termed as "IT Assets". These may or may not be as per the definitions of Finance but require protection and security and may be audited.

1.6 Governance

1. Symbiosis Society is the parent organisation that invests in the IT infrastructure across all its campuses and premises and is its owner. Managing Committee of Symbiosis Society, the highest governing body responsible for policy formulations and management of the institution has delegated the authority for conduct of routine functions to the Principal Director.

Principal Director shall constitute an IT Committee comprising of IT experts within the Symbiosis Family and limited number of technical experts from outside to approve major IT plans and IT procurement and to carry out any IT related activities assigned in the interest of professional planning, procuring, implementing, maintaining or using of IT for smooth and efficient functioning of academics and administration. Chief IT will be

ex officio Member of this committee.

2. Chief IT shall constitute a Technical Cell, consisting of internal experts and appropriate technical experts as and when required, under his/her Chairmanship. This Cell shall carry out technical scrutiny of plans and proposals and submit its findings to the IT Committee for taking final decisions.
3. Chief IT shall be responsible for maintaining requisite records pertaining to basic IT resources and infrastructure for connecting various campuses and premises; and communicating electronically across and outside. All institutes/Departments shall provide material pertaining to such infrastructure and update any change.
4. Chief IT will be responsible for all IT resources at Symbiosis Society including SIU .
5. Directors of Institutes shall be responsible for the IT infrastructure and resources within the institute. For any connectivity across institutes or departments and outside the concerned institute or for any common IT systems, the Director shall carry out its planning and implementation in consultation with Chief IT.

   The Director of an Institute shall assign a suitable senior member of the institute to be IT-In-Charge (IIC) who shall be responsible for administering and maintaining the IT infrastructure of the institute. The Director shall intimate the name and the designation of IIC to Chief IT after assigning a person. In case IIC requires any technical expertise, it shall be sought from the IT Department.
6. Heads of Institutes and Heads of Departments shall assess requirements, plan and make proposal for acquiring IT resources for their respective institute/department except for those common IT systems identified by the IT Committee. Chief IT shall plan and make proposals for acquiring common IT resources and systems identified by the IT committee, including any IT Infrastructure for connecting new or existing campuses or premises. Such proposals shall be evaluated and approved by the IT Committee.
7. Policy decisions as well as Rules and Regulations regarding IT, framed by Symbiosis Society will be published by IT Department of Symbiosis Society. IT department of the Society will be responsible for the implementation of IT Policy. In case of dispute in interpretation, the interpretation of rules and regulations given by Principal Director will be final and binding.

2. Policy on IT Infrastructure and Its Management

2.1 IT Infrastructure at Symbiosis

1. Symbiosis Society aims to acquire, use and maintain its IT assets similar to any other valuable asset of Symbiosis. It is therefore incumbent on those responsible for these assets to assess requirements, acquire assets, use them for the purpose they were acquired for, maintain them and protect them.
2. These policies shall cover the following activities regarding IT assets and shall be detailed separately.
    a. Planning and Procuring
        i. Computing Hardware including servers & PC's
        ii. Networking Devices
        iii. Standard Software Packages
        iv. Customised IT Applications
        v. Other IT Resources
    b. Installing, Managing and Operating
    c. Users and norms for using
    d. Maintaining and Security
    e. Scrapping
    f. Any other function as approved by the IT Committee

3. Heads of the Institutes and Departments are responsible for following all guidelines and procedures laid down by Symbiosis from time to time for all activities from planning to scrapping.
   The major goals of the institutes shall be to provide enrichment of and ease in academic delivery and accordingly the institutes are entrusted with the responsibility of making the best use of the IT assets.

2.2 IT Initiatives

2.2.1 Green IT

Symbiosis aims to imbibe the spirit of Reuse, Reduce and Recycle in using IT. The Green IT policy of Symbiosis encompasses 3 areas: Daily operations, Equipment Procurement and Equipment Disposal.

2.2.2 Policy on Cloud Computing and Open System

1. Symbiosis intends to consider cloud computing for availing the service and utilising its benefits in near future since the demand for Hardware augmentation is growing rapidly. It will help in minimizing the investment in the capital items, reducing the management problems of maintaining growing number of Hardware items, obsolescence of equipment owned and getting latest technology from the provider. Since, most of the cloud services are charged "pay as you use" basis, there is considerable saving in the capital expenditure.
2. The IT Committee shall assess availing any of the cloud services be it Infrastructure as a Service (IaaS) or Software as a Service (SaaS) based on which a detailed policy shall be arrived at.

2.2.3 Business Continuity Planning (BCP) and Disaster Recovery (DR)

BCP and DR as a policy are essential for the Governance of IT Systems. The Heads of Institutes/Departments will be fully involved in implementing it along with the IT Department. At this stage, the policy is to understand the concept, spread awareness and make plans for implementation of this important function.

A Governing Committee will be constituted to develop policy direction, guidance and identification of a team to implement its plans.

2.3 Symbiosis Network

Symbiosis shall build an enterprise-wide "Symbiosis Network" across all campuses and premises to provide connectivity and a secure channel to communicate or transfer

data or access centralised systems or consolidating systems. Institutes may build their own local networks and shall connect the Institute Networks to Symbiosis Network when it is operational.

2.4 Computer Labs

A computer lab is an area equipped with computing devices primarily for the purpose of carrying out academic activities by students and faculty. A larger computer lab may have a network connecting all the computing devices in an Institute along with a server. If the IT load of an Institute demands more than one server and advanced network devices, a separate Server Room with requisite infrastructure will house such equipment. A Server Room should be planned in consultation with IT Department.

2.4.1 Institute Lab

1. Computer Labs may be established by an Institute imparting education with the primary purpose of delivering academic contents and enhancing learning experience, after scrutinising the requirements thoroughly.
2. Institutes shall specify its own requirements for setting up a Computer Lab with or without the technical assistance of the IT Department, using the following parameters in addition to the justification for detailed specifications:
    a. A computer lab configuration should be considered after identifying the programmes with subjects requiring use of computers and software. However, the same lab should be used for maximum number of programmes and as far as possible for maximum working hours.
    b. Out of such programmes, the programme with the largest batch size should be considered for estimating the number of terminals.
    c. In case students are expected to use their own laptops for academic delivery, appropriate facilities should be provided in the lab. Accordingly the number of terminals should be reduced. However, laptops with only legal operating systems and legal software, if applicable, shall be allowed to be connected in the computer lab.
3. For technical specifications of a computer lab, assistance of IT Department may be taken.

2.4.2 Department Lab

1. Departments that are required to handle a large number of transactions and/or to maintain records for statutory requirements and/or to maintain confidential data may be allowed to establish a Computer Lab.
2. In such cases IT department shall scrutinise and assess their full requirements. They shall assist the department in all technical aspects. The Department shall make a proposal in consultation with IT Department.

2.4.3 Campus Lab

1. Symbiosis is in the process of setting up central facilities of "IT Resource Centre" at its campuses for training the employees in Computer Skills and Applications.

2.5 Classroom IT Resources

1. Symbiosis encourages use of technology for contemporary methods of teaching and learning at its institutes.
2. Requirements of display devices and network connectivity for classrooms may be fully assessed while planning IT resources. Once acquired, use of these resources should be promoted among the faculty. As far as possible, institutes of higher education may consider equipping selected classrooms with IT resources based on the requirements of programme delivery.

2.6 Hostel IT Infrastructure

1. Symbiosis shall provide technically appropriate IT infrastructure to Symbiosis hostels whether owned or on hire.
2. Chief Administration shall be responsible for the IT infrastructure at all hostels. Campus Administrator shall be responsible to maintain and administer the same at the concerned hostel/s.
3. A hostel network may be independent from an institute network.
4. Symbiosis shall provide a fixed size of bandwidth to a hostel calculated as per allocation norm per student as approved by the IT Committee. For any additional bandwidth requirement, a student may arrange the same at his/her own cost.

5. The institute bandwidth should be diverted to the hostels at night time to augment or provide bandwidth at the hostels if the existing network design permits. The design of all future networks of any institute should have this facility. This will ensure that the bandwidth is optimally used round the clock.
6. In general, the internet connectivity in hostel rooms shall be provided through cable connectivity and not by using wireless access points, and with requisite security measures such as firewalls etc.. The wireless access points in hostels should be used to provide internet access in corridors and common areas.
7. The IT resources provided in the Hostels are solely meant for academic purposes.
8. Symbiosis is in process of finalising a bandwidth allocation policy for hostels.

2.7 IT Resources for Employees

1. Institute may assess role and workload of an administrative function and allocate a desktop to an employee performing the role.
2. Institute may procure laptops or portable devices for a functional requirement provided with adequate protection from hazards arising out of its portability.

2.8 IT Code of Conduct

1. Symbiosis is a responsible educational organisation and shall install legal IT assets at all its campuses and premises.
2. Symbiosis employees are directed not to install any unauthorised or unlawful IT resource on Symbiosis IT systems.
3. Symbiosis employees shall not misuse or disclose any official data or information to third party without written permission.
4. Students of Symbiosis shall use the IT systems solely for the purpose of learning and research.
5. All users have responsibility to protect IT resources for which they have access or custodianship.
6. Symbiosis employees are accountable for their access to and use of the IT Resources at the concerned Institute or Department. They will not share their access keys or User IDs and password with another individual. In exceptional cases, User IDs and passwords may be shared with the permission of the Head to meet any exigencies. In such cases the person to whom the User Id belongs shall be responsible for its

legitimate use.

7. No users shall load or host or access any indecent or unlawful material on Symbiosis IT resources. They shall not connect to any unlawful device or access prohibited sites or carry out any unlawful activities on the internet or any Symbiosis network. The Internet Policy of Symbiosis shall apply.
8. All users are bound to follow all security norms laid down by the IT Department and the Institute.
9. Resources or systems owned and maintained by Symbiosis for the benefit of the academic community are primarily intended for use of Symbiosis, not personal or business communications.
10. Institutes and Departments may adopt additional information technology policies that are specific to their operations, provided that such requirements are consistent with this Policy and the Institute/Department provides a copy of the same to Chief IT. In case of inconsistency, the provisions of this Policy will prevail, unless the Institute/Department specific policies are necessary to meet legal requirements governing certain types of information, in which case the more specific legal requirements and related policy will take precedence.
11. None of the users of the IT facilities shall indulge in activities that violate the prevalent Cyber Law of the Government of India.
12. Any breach of this code shall be deemed as indiscipline and may attract commensurate punitive actions.

3. Policy on Computer Lab Administration

3.1 Purpose

1. The main purpose of a computer lab is to facilitate learning by students using IT resources.
2. This policy shall provide a systematic approach for
    a. management and operations of Computer Lab in order to ensure, prompt response to user needs, streamlined operation and high performance;
    b. effective coordination with all relevant stakeholders with the aim to ensure high availability of systems & networks to the satisfaction of end users.

3.2 Applicability

1. This policy applies to an institute or a department that establishes a Computer Lab. A Lab Team comprising of internal and/or external technical personnel shall implement this policy under the guidance of IT-In-charge.
2. It shall carry out the following
    i. monitoring of systems performance
    ii. maintenance and operations of all equipment, and
    iii. management of assets & resources.

3.3 Monitoring Systems Performance

1. The Computer Labs of Symbiosis shall function to ensure high uptime for the servers and network including various equipments such as switches, servers, desktops and workstations and various external services.
2. Monitoring of the Computer Lab shall constitute:
    a. Checking of logs of various systems and identifying deviations from norms
    b. Inspection for faults of all IT resources inside and outside the Computer Lab,
    c. Checking performance of various servers and network systems as per the SLA agreed with the service provider
    d. Checking back-up logs and records.

3. The Computer Lab staff shall maintain Daily, Monthly and Annual monitoring routines. Broad guidelines and training for the same shall be provided by IT Department from time to time.
4. IT-in-Charge shall be responsible to monitor system performance on a regular basis.
5. IT-in-Charge shall take appropriate corrective actions so as to bring the system at the expected level of performance.
6. IT-in-charge shall also monitor services provided by the contracted vendors/service providers for the agreed performance SLA's for the services provided.
7. Technical person/s supporting the Computer Lab shall be familiar with monitoring, inspection and first line repair of the equipment. An Instruction Sheet for checking equipment status shall be on display at appropriate places.

3.4 Operations and Maintenance

1. An Institute shall systematically administer the main functional units of its Computer Lab viz. Network Management, Server Management, Software Management and Data Management and Facilities Management (UPS, Air conditioning etc.).
2. An institute shall maintain control sheets for each of the functional units as per the guidelines given by IT department.
3. An institute shall protect all IT assets such as hardware and network from physical hazards; and establish network security, data and software security with appropriate security measures. As far as possible, a computer lab should be equipped with CCTV cameras for physical security.
4. An institute shall record the performance related data and analyse them periodically as per the norms set by the IT department. For any technical expertise, assistance of IT Department may be sought.
5. Each Computer Lab shall schedule maintenance of IT equipment depending on its usage, criticality or manufacturer's guidance. Typical monitoring schedules shall be provided by the IT Department.
6. As far as possible, first level maintenance of out-of-warranty IT resources, shall be carried out by the in-house Computer Lab team.
7. IT-in-Charge shall ensure that all requisite contracts for annual maintenance with approved contractors are operational, for the IT resources that are not under warranty.
8. For critical IT resources that are not under warranty and are expected to perform

continuously, Annual Maintenance Contracts (AMC) should be entered into with approved and competent vendors in consultation with IT Department.

9. If any IT equipment is not under warranty or AMC and requires expert services for desired performance, a competent vendor should be engaged in consultation with IT department.
10. In case of shortage of competent technical manpower required in a computer lab, competent services of authorized vendor may be obtained in consultation with IT Department.
11. Regular monitoring, coordination and communication shall be maintained by the technical staff with other support services of Facilities Management such as Electrical & UPS services, air-conditioning and fire & safety services.

3.5 Management of IT Assets

1. An institute shall maintain "Asset Register" viz. a comprehensive list of IT resources and equipment and their locations along with other data as required by the statutory authorities at all times.
2. Whenever a new IT asset is acquired it should be recorded in the IT Asset Register.
3. An IT asset may be moved or transferred only with the authorisation by the concerned Heads. Whenever any IT asset is required to be shifted, within the Institute, between the Institutes or between the Campuses, the correct status and location should be entered in all relevant IT Asset Registers.
4. An annual inventory of all IT assets and periodic physical verification of the assets shall be carried out as per the guidelines issued by Finance Department and IT Department.
5. The planned replacement of an asset based on its usage and life-cycle shall be carried out at proper time as per the obsolescence policy.

3.6 Green IT in Daily operations

1. There should be minimum wastage of electric power. Only the necessary light points and fans should be switched on and those not required should be powered off consciously. Similarly the equipment not required should be kept in powered-off state.
2. Air conditioning (AC) should be kept running mainly for operational and

environmental purposes.

3. It is mandatory that projectors, AC, fans and lights as well as all devices including desktops and printers in the user area should be powered off, when not in use.
4. As far as possible racks in a server room should be designed to avoid uneven flow of air conditioners so as to lessen the demand of cooling by the equipment.
5. Printing on paper should be avoided as far as possible. Printing should be done only in cases when material is final and needs to be submitted or retained as a hard copy. Printed material if confidential should be shredded and in all other cases attempts should be made to reuse the old discarded printed stationery. Print monitor software has to be installed for better governance

4. Policy on Computing Hardware & Peripherals: Servers, Desktops & Personal Devices

4.1 Purpose

The purpose of this policy is to define standards, procedures, and restrictions for the servers installed on institute's internal network(s), desktops or personal devices. It aims to reduce the operating risk and server downtime.

4.2 Applicability

1. This policy is applicable to any Institute or Department installing and managing any computing hardware and covers all types of servers including those servers connected to internet services, which are owned, operated and controlled by Institute/Department.
2. Computing hardware includes servers, desktops, personal devices, peripheral devices etc. Servers, Desktops, Printers have a fixed location in an institute whereas the personal devices like Laptop, Mobile phones, PDA etc. are portable. This policy provides basic guidelines for connecting these devices.
3. Allocation of any server to a particular user group may be decided as a local policy of the institute or department.

4.3 Servers

4.3.2 Types of Servers

1. The most commonly installed servers in Symbiosis are:
    a. **Internet servers:** These are servers connected to internet services provided by an Internet Service Provider (ISP). For example, FTP servers, Proxy servers, etc.
    b. **Application servers**. : On these servers customised applications or application packages used for administering academics or other functions are hosted.
    c. **Database servers:** are the servers on which data is maintained in a database management system (DBMS). Apart from DBMS data, these servers may also host data on spreadsheets, important documents etc. required for statutory purposes and official administration.

d. **Web Server:** hosts the institute website
e. **Mail Server:** hosts email services of the institute.
f. **Any other server** catering to specific requirements.

2. More than one or all servers may reside on the same hardware depending on the volume of transactions and requirements of an institute as determined in an optimal way.
3. An Institute may decide to use external servers which are maintained by third party or a Data Centre or on Cloud. Such services may be procured by an Institute/department as per the prevalent Procurement Policy of Symbiosis.

4.3.3 Management of Servers

1. IT-in-Charge (IIC) of an institute shall be responsible for proper installation, configuration, monitoring and security of servers as per the standard procedures and ensure continuous and efficient functioning of servers.
2. The configuration of a server, operating system and any other supporting software required by the server will be specified by the Institute at the time of procurement. These specifications shall be approved by the IT Committee after technical scrutiny, at the time of its procurement.
3. In the subsequent period if any upgrades are required to an existing server, the institute shall detail the specifications in consultation with IT department to conform to the norms. The institute may place its proposal for upgrading a server through the normal process of procurement.
4. Each and every server shall be either under Warranty or under an Annual Maintenance Contract (AMC) with an approved vendor having expertise in maintaining the server configurations. IT department will maintain a list of approved vendors after ascertaining their expertise and experience of providing efficient support for maintaining AMC of Servers and other devices. All institutes shall utilise the services of an approved vendor for maintaining their servers.
5. At the time of installing a new server, the Institute shall obtain “Service assurance certificate” from the concerned vendor.

4.3.4 Guideline for Server Administrations

1. An institute shall maintain a document describing established standards and guidelines for the server administration including those issued by IT Department.
2. Some essential guidelines are:
    a. OS configuration must be in accordance with *Standards and Guidelines* for *Server Operating Systems.*
    b. Services and applications that are not required any more must be disabled or uninstalled, with the approval of the Head.
    c. Access to services must be logged or protected through appropriate Access Control methods.
    d. Security patches must be installed on the server system regularly to keep the servers up-to-date.

4.4 Desktops

1. When an Institute acquires a desktop it shall be allocated for specific use as per the direction of its Head.
2. A desktop may be allotted to an employee for official work and the employee shall be the custodian of the same. The employee shall be solely responsible for maintaining any data, message, mail or any other content as per the IT Policy.
3. Every desktop shall have an asset number. It should be recorded in the Asset Register along with physical hardware tag number, the logical address of the device and also to whom it is allocated. Any allocation, reallocation and/or relocation of a desktop shall be properly recorded, whether connected to the Institute Network or not.
4. A device may be connected to the Institute network after taking care of standard security measures. For connecting to the network, a desktop or a personal device shall have applicable and compatible legal operating system and antivirus software.
5. Access to any application may be permitted to facilitate official work.
6. The user shall not install any software without the approval of the Head or change the setting of the control and other sensitive details without the supervision of the technical staff.
7. Before using any external media on the desktop, a user must ensure that it is free from any virus.
8. Users should be instructed to keep official and personal data separately.

4.5 Laptops and other Personal Devices

1. Symbiosis may provide laptops and personal devices to Heads/Directors and to persons identified by the Head/Director for carrying out their normal duties in an efficient manner. Normally a laptop is allocated to individuals who are mobile or who need to carry out their duties while on the move. An institute/department will seek an approval for the number of such devices to be allocated to their employees or for common use from Principal Director.
2. Laptops (instead of desktops) may be given to faculty who are UGC qualified and have been appointed through the regular selection process as full-time faculty.
3. Faculty appointed through the ad-hoc process and adjunct faculty will be given a desktop only and not a laptop.
4. Research assistants/associates and Teaching assistants/associates will be given desktops only and not laptops.
5. Each personal device must be registered by the name of a user and Mac address. The systems administrator shall control this activity of registration.
6. Network Administrator or a senior technical staff in the absence of Network Administrator shall be the custodian of the portable devices commonly used in the Institute. He/she shall issue such a device on approval by the Head to a user with a proper log of issue and return.
7. All such devices belonging to the Institute should be stored in a secure place. The Lab staff shall ensure that such a device has an Asset Identification number and is kept in state of readiness for its use at any time.
8. The individual who is allocated a portable device will be responsible for the safety and appropriate use of the device.
9. A user's laptop may be allowed to access internet, based on the requirements as approved by the Head of the institute. If the device is allowed to access internet through the Institute domain, it must be configured for, by the Network Administrator.

4.6 Antivirus Policy

Symbiosis intends to protect the IT systems from any virus menace. A virus can be transmitted via e-mail or instant messaging attachments or downloads or external media. This policy is to take measures and implement best practices for eliminating risks of a virus attack.

1. The institute shall install licensed copies of anti-virus software on all systems. The most recent version of the anti-virus software package will always be used for installation.
2. The antivirus software must be active and up to date at all times. Technical staff should carry out virus checks routinely on all systems.
3. All users shall be responsible to ensure that virus infected software or media are not installed or read at any time. Email attachments may be downloaded only if cleared by the anti-virus software.
4. No portable device shall be connected to any Symbiosis network if it is not cleared for virus.
5. A user who is allowed to connect his/her laptop to the Institute Network shall hand-over the laptop on demand by the technical staff for Antivirus scanning or for any other security measure, if required. Institute technical staff shall advise the user to save any important files prior to carrying out virus checks.
6. The Institute should continually communicate about any virus threats to all users.

5. Policy on Network/s

5.1 Purpose

In Symbiosis the network/s is comprised of Local Area Network (LAN) and Wide Area Network (WAN). Both are similar in their management and operations while technically different. This policy is related to both types of networks and aims to streamline management of connectivity, high uptime, response and performance of the networks.

5.2 Applicability

This policy is applicable to all Institutes/Departments which have installed Local Area Network and have liaison with a service provider for internet or connected with a software application installed at its vendor's site.

5.3 Networks

5.3.1 Administration of Networks

1. Symbiosis intends to ensure that all networks whether Institute Networks or Symbiosis Network, shall have fault free operation, high uptime and security from intrusion and hacking.
2. Network Administrator of an Institute/Department is responsible for managing its network and ensuring that the reliable connectivity exists to the Symbiosis network. In case a network administrator requires technical support other than that is regularly provided, he/she shall obtain expert technical services in consultation with IT Department.
3. The Head of an Institute/Department is the authority to approve access to a user, depending on the requirement of user's role or task.

   For example, Accounts staff of an Institute will be allowed access to Finance Systems and emails while the students may be restricted to the academic systems only.
4. A Network Administrator shall provide network access to a user as approved by the

Head of Institute/Department. Any ad-hoc or temporary access may be provided with explicit permission of the Head and only for a specified period. For example, for a research assignment, the Head may approve access to normally not accessible sites to a user for the period of the assignment.

5. A Network Administrator shall maintain an up-to-date cable routing and network layout diagram. The network diagram should represent actual on-ground layout of the equipment and the current configuration of the network. A printout of the basic network diagram should be displayed at a prominent place in the server room.
6. The server room should be accessible only to authorised persons. Entry to the server room should be recorded in a Register or recorded electronically.
7. No equipment will be connected directly or over WLAN to the managed network resources.
8. Whenever there is a change of Network/System Administrator at the Institute or Hostel/Campus, the Handing Over and Taking Over documents must be submitted to IIC with a copy to the Head and the IT department.
9. The IT department shall maintain details of the network of each institute as submitted by the Network Administrator from time to time.
10. For Hostel Network Administration, in case of shortage of technical manpower, the Institutes to which hostels belong should extend support.
11. IT department shall organise training of technical staff periodically to equip them for improving management of the networks and IT resources and to keep the staff up-to-date with technology.

5.3.2 Connectivity

1. A network shall be designed to provide flexibility in connecting equipment and making logical segmentation of the LAN depending on user group, applications etc. This helps maintenance and isolation of any segment logically and restricts its access to specified servers /folders and files.
2. The Network Administrator shall carry out any reconfiguration within the existing setup for smooth operation or better performance of the network. For any major restructuring of the network, IT department should be involved.

3. For any alteration in configuration, Network Administrator shall obtain the approval of the Head. In case procurement is required for such alteration, the normal Symbiosis procedure for procurement should be followed.
4. Institutes are free to create their VLANs as per requirement. The network administrator should assess requirements and create VLAN. For any technical help Network Administrator may contact IT department.
5. A device may be connected to the Institute network at appropriate nodal points including voice/data jacks, and also through an approved wireless network access point. For remote users a device including video-conferencing device may be connected to the Institute via a VPN or SSH tunnel or any other approved network services.
6. The Head of an Institute shall approve connectivity to any external devices to the network, taking into account the overall load on the network and security requirements.
7. Before connecting a mobile device, it should be registered with the concerned Network/Systems Administrator who should ensure that the device has the appropriate security patch on it.

5.3.3 Monitoring of Response and Performance of Networks

1. The network administrator shall monitor the quality of service of the internet provided by the vendor on a daily basis. The quality of service should meet the SLA agreed by the vendor. In case of any non-conformance, the Network Administrator shall follow up with the concerned vendor immediately for bringing back the internet performance to the desired level. In case of a failure by the vendor in meeting SLA, even after repeated follow up, the Network Administrator shall immediately escalate the matter to the IT department.
2. On a daily basis, a network administrator shall check if all the critical components of the network are performing satisfactorily and in case of exception take necessary steps to ensure that the network is fully operational.
3. Regular monitoring of the network shall be carried out at predetermined times. The technical staff should be trained for this purpose.
4. Vital and/or frequently required spare parts of critical network equipment may be

kept in stock for quick remedial action by the in-house team.

5. Network audit shall be carried out periodically, at least once a year. This will help identify improvement areas for the network performance.
6. The IT department will constitute an internal audit team of knowledgeable network administrators and any other experts as required, who will conduct periodic audit of the Institute networks. The audit team visiting an institute will have members from other institutes. All non-compliances shall be attended immediately by the institute concerned.

5.4 Wireless Access and Wireless–LAN (W-LAN)

Wi-Fi technologies are inherently insecure and any unencrypted data sent over such a connection is vulnerable to interception by unauthorized persons or parties. Although the locations of the Access Points (AP) of a WLAN are inside the Symbiosis premises, their range and coverage go beyond. Therefore, without proper security, the APs installed at various locations of the institute's premises can be accessed and the network can be penetrated by an outsider. This may cause loss of information, damage to critical applications, and damage to the public image of Symbiosis.

Wireless access policy therefore aims to ensure a secure, reliable and manageable wireless network.

5.4.1 Administration of WLAN

1. Network Administrator shall be responsible for installation and maintenance of the wireless devices. Any technical assistance, if required, may be sought from IT Department.
2. All wireless access points within the institute firewall need to be centrally managed and configured by Network Administrator and technical staff.
3. An Institute/Department may add new wireless access points within its own network after due assessment of requirements and technical feasibility.

5.4.2 Wi-Fi Configuration

1. Network Administrator should remain vigilant of "rogue" access points being surreptitiously installed without the knowledge or permission of the Institute/Department by constant monitoring of the network through firewall and any other software/s, planned / unplanned survey, coordinating with campus admins to identify untoward incidents on campus etc.

   Such "rogue" APs may be used by hackers, internal employees, or trespassers to gain illegal access to the network and Internet connection for the purposes of sabotage, spamming, corporate espionage, personal gain, and so on.
2. The technical staff shall implement encryption, strong authentication, and other security methods as per the norms.
3. The network may still be vulnerable over the Access Points (AP's) of the WLAN. As far as possible such Access points should be connected to a manageable switch that will facilitate monitoring through the Wi Fi controller.
4. Whenever a wireless device is being connected to the network it should be secured by means of strong wireless security measures such as password, WPA security network key, MAC Id etc.. Wireless security protocols may also be installed on wireless connections.
5. Whether any sophisticated wireless security protocols are implemented or not, Network Administrator should configure the APs so as to allow only the registered MAC Ids. The Access to the network is thus available through any Laptop or own devices only if its MAC address is registered with the Lab. The Network Administrator may block any suspicious MAC Id's.

5.5 Policy on Firewall

Firewall is considered as the first line of defence against external threats. The role of the firewall is to restrict internet access to notified sites and to prevent intrusion into the institute's network by unauthorized entities. Firewall Policy shall describe how the firewall will filter Internet traffic in order to mitigate risks and losses associated with security threats, while maintaining appropriate levels of uninterrupted access for authorized users.

5.5.1 Configuring a Firewall

1. The firewall must be configured to protect the network information such as system names, network topologies, and internal user IDs, from the Internet
2. Access to the network should be given from the trusted and authorised users and should be denied to the untrusted parties from the external networks.
3. Unwanted traffic as determined by the firewall rule-set given by IT department should be blocked.

5.5.2 Operations and Administration:

1. The network administrator shall be responsible for managing the firewall as per the guidelines from IT department.
2. The Network Administrator should monitor the console log for analysis of the traffic to and from the internal network.
3. The Firewall should be configured for strict authentication for the users of the network.
4. The firewall license should be renewed promptly and latest updates on the product should be adopted timely.
5. All Virtual Private Network (VPN)s should be configured through the firewall.

5.6 Policy on IP Addressing

This policy aims to plan and manage IP address blocks for services and devices to facilitate IT governance.

1. An institute will follow a standard procedure for allocation of IP addresses to individual user/s to ensure proper use and designation of IP addresses for all stakeholders, network devices and services. It should conserve this scarce resource and enable more efficient and hierarchical routing through the optimal use of IP blocks.
2. The Institute technical team shall use the following guidelines on IP addresses.
    a. TCP/IP approach for allocating IP addresses should be used.
    b. Private IP subnets should be judiciously allocated (use of DHCP can be mentioned)
    c. Public IP addresses may be shared only with the approval of the Head and a record should be maintained by the Network Administrator.

6: Policy on Security

6.1 Purpose

The security Policy of Symbiosis is to achieve information security in a cost-effective manner. It is framed in consonance with the ISO 27001(erstwhile BS7799) standards and as per the guidelines and deliberations of Information Security Management System (ISMS).

The policy aims at achieving Physical security, Server security, Network security, security of all Information Assets and perimeter security. It lays down a systematic approach for securely managing IT resources and facilities resulting in better performance within given resources.

6.2 Applicability

All Institutes and Departments shall implement the Security Policy of Symbiosis.

6.3 Security Policy

1. **Physical security**:

   The risk assessment of the physical site and equipment should be reviewed periodically to check the electrical, air conditioning systems and the firefighting equipment. The following physical check shall be implemented.

   i. Computer Lab

   a. Entry to the Computer Lab should be restricted to authorized users only.
   b. Users will be allowed in a computer lab only for academic use of lab resources.
   c. No unauthorized visitors should be allowed into the computer Lab without an authorized escort.
   d. As far as possible entry to the Computer Lab should be recorded either electronically or manually.
   e. Users should follow lab discipline in the computer lab and not bring prohibited items such as eatables, beverages etc. inside the lab.
   f. Users shall not mishandle or disassemble any lab equipment.

   ii. Server Room

a. Server Room or the Network Centre hosting network cabling and equipment racks and cabinets should be locked, when unattended by authorized personnel.
b. Visitors to the Server Room must be escorted by the authorized persons.
c. Network cabling and devices should be physically secured wherever possible.
d. Entry to the server room should be recorded with the date and time of entry and departure.

iii. Portable devices of Institute

a. Portable devices such as laptops, iPads etc. should be stored securely when unattended.
b. Important data stored on portable devices should be encrypted. Whole disk encryption is recommended on laptop computers.
c. When traveling with portable devices or using them in public places, appropriate security precautions should be taken to prevent loss, theft, damage, or unauthorized access.
d. Appropriate security measures should be taken while using datacards.

2. Physical assets

i. There should be regular checks on the physical items such as computing devices, networking devices, tools and instruments, media etc... A physical audit should be conducted periodically and the physical assets should tally with the records of Asset Register.
ii. Symbiosis is not responsible for the physical security of personal devices of users.

3. Environmental Security

i. Electrical power

a. Electrical power for servers/network equipment should be backed by uninterruptable power supplies (UPS) to ensure continuity of services during power outages and to protect equipment from damage due to power fluctuations.

b. Each UPS should have sufficient capacity to provide at least 30 minutes of uptime to the servers and the network connected to it and should be protected with a standby power generator for continuous supply wherever necessary.

c. Desktops may be provided with UPS power supply either centrally or stand-alone mode, for at least 15 minutes.

ii. Fire Fighting

a. Operational readiness of the fire-fighting equipment in the computer lab should be maintained at all times.

b. All IT staff should be fully trained in managing the fire-fighting equipment, especially in the computer lab.

4. Network Security

i. Any network of Symbiosis must be protected with a firewall ensuring intrusion protection system (IPS) and intrusion detection system (IDS) adhering to Network Policy of Symbiosis.

ii. For transmission of data on the network, data encryption should be followed as per the guidelines of IT Department.

5. Server Security

i. Apart from physical protection of the server, timely configuration of the operating system should be carried out incorporating latest patches released by the vendor.

ii. Whenever virtualisation is carried out on a server, the security requirements on the hypervisor must be met.

iii. Servers must be formatted in regular basis after taking proper backup of data. This must be done once in a semester

6. Access control

The policy attempts to balance restrictions on unauthorized access to information and services against the need of authorized users.

i. **User Notice** - Before a user accesses the facilities of an IT system, a notice should be displayed that warns against unauthorized use of the IT resources or IT system.

ii. **Remote access** - Remote access should be controlled through appropriate identification, authentication, and encryption techniques.

7. Identity Control

i. In order to prevent identity thefts, Institute/Department should register only bona-fide users with a Symbiosis id. This should be associated and controlled with a proper domain name.

ii. Institute must take maximum care for establishing **password control** and the specified password policy should be adhered to.

8. Security on Vendor Products

i. A vendor should specify how an IT product supplied meets the security requirements of this policy and any special security requirements of the system. The vendor must allow testing of the system's security controls by Symbiosis or an independent third party, if needed.

ii. Any demonstration or testing of an IT product should be carried out only on test data that mimics the 'live' environment without accessing the 'live' systems.

9. Incident Reporting

i. **Security incidents:** Any user who suspects that a security breach has occurred must report the incidents to Network Administrator/Systems Administrator of the Institute immediately.

ii. **Responding to Security Incidents**

Network Administrator/Systems Administrator shall evaluate the level of severity of the reported incident and escalate the incident to IIC and the Head of the Institute depending on the severity. They will arrive at corrective measures in consultation with IT Department, which in turn, may decide to circulate the incident along with remedial measure to other Institutes/Department, if applicable.

10. Handling of Media

i. Disposal of Media

a. Whenever any IT media is to be disposed of, it is necessary to ensure that all Symbiosis Data are properly erased using the appropriate commercial tools to erase the data in such a way that it is irrecoverable in all circumstances.

b. If equipment that can store Symbiosis Data, such as desktop and laptop computers or external hard drives is to be disposed of, all data storage devices should be removed before disposal.

c. An assurance should be obtained from the vendor collecting scrapped media that the media will be physically destroyed complying with the environmental laws.

ii. Data Purging on Media

a. Electronic Storage Media (hard disk drives in computers, external hard drives, USB flash drives, magnetic tapes, etc.) that will be reused within the Institute / Department should have all Symbiosis Data purged to prevent unauthorized disclosure.

b. If purging is done by overwriting the data, the *entire media/device* must be overwritten with a minimum of three passes.

11. Awareness & Training:

a. An Institute shall train a new member of the Computer Lab on lab procedures, security policies, its implementation and procedures for handling jobs.

b. The Institute shall maintain up-to-date documentation for reference by any concerned member.

c. The Institute shall also spread security awareness among its users.

12. Audit & Control Measures:

The Network Administrator shall monitor the network for security and report any lapses to IIC for taking corrective actions by concerned members. Security audit shall be a part of the network audit by the Audit Team formed by the IT Department. Any non-conformance reported by the Audit Team shall be addressed by the Institute with a corrective action.

6.4 Policy on Passwords

The aim of the password policy is to ensure authenticated access to IT resources and information systems.

6.4.1 Administration of Passwords

1. An Institute shall lay down a safe and secure procedure for allocating password for computing devices, network devices, servers, systems software, application software, database systems and other IT systems wherever applicable.
2. A Systems Administrator or an authorised person from the Lab team shall be responsible for managing passwords.
3. Approval by the Head is mandatory for connecting any personal device to the institute/department or hostel network. The device must be registered by recording details such as Mac id and other device details for providing network/internet access.
4. All critical passwords must be written clearly on a paper which should be put in an envelope marked “confidential” and sealed. It should be kept under the custody of a senior authorised member and the Head of the Institute. Only on specific requirement, the envelope should be opened with the approval of the Head and the passwords be used. Subsequently it is important to change the passwords and the updated list be handled in the similar fashion.
5. Sharing of passwords should be prohibited.
6. Password with global access must be authorised by the Head of the Institute.
7. A password shall be structured as per the guidelines of the IT department.
8. IIC shall maintain confidential record of security passwords of all desktops allotted to the employees, for use in exigencies. The employee shall ensure that a confidential record of any change in security passwords is provided to IIC.

6.4.2 Non-Compliance of Password Policy

Not following the password policies or procedures should be considered a security breach. Depending on the nature of lapses, various sanctions may be imposed by the Head of the Institute whose decision shall be final.

7. Policy on Data Administration

7.1 Purpose

Critical and confidential data pertaining to the academic bodies and other stake holders are generated and maintained at Symbiosis in day-to-day operations. It is essential to ensure authorised data access, retrieval of authentic data and prevent any breach or leakage of data from the storage media. The policy specifies guidelines for data organisation, data handling, data back-up and data security in order to meet various requirements of Symbiosis.

7.2 Applicability

This policy applies to the storage of data generated and stored across all Institutes and Departments using any IT facilities.

7.3 Data Organisation

1. All data created through IT systems shall be stored in a systematic manner on servers or desktops or any other storage device.
2. Standard Naming conventions shall be used for files and folders so as to allow easy official access. Such naming convention shall be recorded with IIC. For example all files related to Examination section should have file names starting with EX; all file related to Admissions to start with AD etc..
3. Data folders on servers required for running the systems shall have standard names as per the guidelines of IT Department.
4. System Administrators shall be responsible to ensure that data from all the servers and network files are maintained in a standard fashion so that the system services do not suffer even when there is a change in technical staff.
5. Each institute will maintain official data on the data server. Any data considered as official must be first recorded on official data server prior to releasing it to the concerned person or organizations. An Institute shall create folders for major functions and maintain year-wise data within the concerned folder. Typically an institute may have official data folders such as Admission, Academics, Finance, HR,

University, Purchase, Statutory Bodies, Accreditation etc. By organizing data in this manner it should be possible to obtain historical data of any function for statutory or any other purpose.

6. Under no circumstances official data shall be maintained on the local storage of an individual employee. An employee may maintain relevant data on his/her hard disk for working purposes and shall submit the finalized data that is to be officially released to the official data server.
7. All official data of confidential and sensitive nature must be stored in a separate folder the access to which should be controlled by the use of a password available only to authorised persons.
8. The Head of an institute/department along with those functionally responsible shall define a Data Retention policy based on criticality and statutory requirements. The statutory requirements may be obtained from the Functional Heads of the Society or the Registrar of the university as the case may be. This shall be audited during an IT Audit.
9. An index of all official data folders should be maintained as confidential and should be communicated to senior authorities in the institute/department.

7.4 Data Handling

1. Only those employees who are responsible for official functions shall handle any data related to the function. Any other user required to use that data shall be authorised to read or update according to the requirement assessed by the functionally responsible employee with the approval of the Head.
2. All confidential data shall be maintained separately and should be accessible only to the authorised users.
3. All critical data should be handled with restricted access. Only persons designated by the Head of an Institute/Department should be allowed to view and work on them.
4. Any data required for statutory purposes shall be maintained appropriately for the prescribed period. Care should be taken so as to ensure that such historical data is accessible as and when required. A proper back up procedure must be followed which allows to save data at two different locations with appropriate recovery time and recovery point objectives.

7.5 Data Backup

1. Systems Administrator shall schedule daily back-ups, monthly back-ups, event-based back-ups(e.g. on closing of the financial year, announcing the results of a semester), annual backups (for the annual cycle of an enterprise application system such as HR data on 31st Dec and 31st March, Finance on 31st March & 30th Sept, Academics depending on academic cycle normally on 30th of Apr.) etc.. based on the requirements of the Institute/Department.
2. Systems Administrator shall ensure that backup procedures are carried out to satisfy the Data retention policy. While re-cycling any storage media, care should be taken that no vital data is lost.
3. All back-ups, either manual or software driven, should be carried out by the designated person. The storage of such data should be indexed and maintained by the designated person with details about content, location and indexed storage media for that content.
4. The information for general back-up must be maintained manually in a register or in a software based system, where the media location be indicated for each back-up cycle.
5. Wherever standard database systems relational or otherwise, is installed, the institute should have the services of a trained database administrator.
6. All archival data should be properly backed up for easy retrieval.

7.6 Data Security

The data security of Symbiosis, in essence, attempts to establish the maxim of IT security that is Confidentiality, Integrity and Availability of all data. Some aspects are covered in the earlier parts related to data organisation, handling and data back-up to ensure availability and maintaining integrity. The policy is further elaborated in the next few pages.

1. Data Classification and Security

The Head of Institute/Department shall use his/her discretion to decide the proper classification of any data/ information as defined here.

i. ***Confidential*** information includes sensitive personal and institutional information. Such data may be encrypted as needed. Disclosure of such sensitive information to unauthorised parties should be considered as severe violation of Symbiosis work ethics. Institutes/Departments shall establish appropriate protection against unauthorized access, modification or destruction of such data and information. Special back-up procedure should be implemented for this class.

ii. ***Internal*** information includes operational data/information that is critical for running the functions of Symbiosis and if exposed to unauthorized parties, may have an indirect or possible adverse impact on interests of Symbiosis. Institutes/Departments shall establish appropriate procedures to avoid internal abuse of data.

iii. ***Public*** information is information that may be published or available to the outside world and has no material adverse impact on the interest of Symbiosis on such disclosure. It is encouraged to publish such data that may enhance the reputation of Symbiosis. Institutes/Departments shall ensure that such data is accurate, up-to-date and is protected from corruption and defacing.

2. Data Loss Prevention

Symbiosis considers it important to carry out secure management of the data it holds and generates. Any inappropriate mismanagement or loss of it can harm its functioning. If any employee identifies any loss or leakage of data, the incident should be reported to the Head of Institute/Department who in turn should assess risks of such losses and take appropriate measures to restore the data and prevent such incidents in future.

3. User Responsibility

A user shall be responsible for complying with all security-related procedures for data/information to which they have authorized access or any data/information hosted on the device that is allotted to the person.

8. Policy on Obsolescence & Disposal

8.1 Purpose

Symbiosis adds to its IT Assets and also upgrades them according to the requirements of Institutes/Departments. Several of its assets become obsolete due to change in technology or usage or degradation of its performance or the end of useful life of the asset. This policy addresses on how such cases should be identified and treated.

8.2 Applicability

This policy applies to all IT assets acquired, used and maintained across all Institutes and Departments using IT facilities.

8.3 Identifying Obsolete Assets and Disposal

1. An Institute or Department shall constitute a committee for Obsolescence and Disposal of IT Assets, chaired by the Head and comprising of IIC, Network/Systems Administrator, Admin Officer and Accountant as members and any other competent Symbiosis employees chosen by the Head.
2. The committee shall meet prior to preparing an annual budget of the Institute/Department.
3. The committee shall review the list of IT assets proposed for obsolescence by the Network Administrator/Systems Administrator. The list should also contain justification for obsolescence of each item.
4. The committee will judiciously take into account feasibility to extend the usage of an asset and decide on whether to make an asset obsolete or not.
5. The committee will also recommend disposal mechanism for each IT asset finalised for obsolescence.

8.4 Obsolescence

1. An IT asset may reach obsolescence due to reasons such as:
    i. change in technology
    ii. damage due to heavy usage or inappropriate environment
    iii. degradation of its performance
    iv. reaching the end of useful life
    v. lack of maintainability on withdrawal of the product by the manufacturer
    vi. Any other reason - must be clearly specified
2. Over a period of time, it is observed at Symbiosis that:
    a. Desktop Computers have 4 to 5 years of life,
    b. Laptop Computer have 3 to 4 years of life, and
    c. Servers have 5 years of life.

   This is only an indicator and should not be taken as a standard for obsolescence.
3. When a manufacturer of an IT product withdraws its support, the committee should assess its useful life and maintainability without the support of the manufacturer. If it is not maintainable then its disposal should be considered in a phased manner.
4. The lifecycle of an asset can be extended for two or more years by bringing down its usage.
5. In some cases, obsolescence may need to be considered before the end of the lifecycle of an IT asset. For example, even if a firewall is well within its life span, the security threats from the external environment on the network may demand better technology to protect the in-house system.
6. The estimated life expectancy may be ignored in following cases:
    a. Frequent Failures of the Equipment.
    b. Software requiring higher hardware configurations with certain capacity and performance capabilities.
    c. Reconfiguration of Systems and Networks.
7. All options of continuing with the asset till its services could be fully utilised should be considered.
8. In-house support can also be utilized to support the IT product after the end of lifecycle.

8.5 Disposal

8.5.1 Options for Disposal

When an IT asset is identified for disposal the following options may be considered.

1. **Work with local schools:** Symbiosis can partner with local schools by donating an obsolete asset but in good condition for their use or technology projects.(after appropriate data cleansing operation is performed)
2. **Use older equipment for training and testing:** Those assets that are still in good condition can be used for testing purposes in labs.
3. **Cannibalize:** Parts of obsolete assets that are in usable condition, can be used as spare parts if they are compatible with other equipment. Replacement disk drives are a good example.
4. **Buy-back:** If possible the old equipment may be traded for newer equipment provided reasonable discount can be obtained.
5. **Sell or auction older equipment to employees:** Institute may consider offering the obsolete equipment if in good condition to its employees at a low cost after clearance from Symbiosis Finance/Administration.
6. **Donate to charities:** The obsolete IT assets that are in good condition can be donated to charitable organisations after clearance from Symbiosis Finance/Administration.
7. **Sell as scrap:** If none of the disposal options above is feasible this should be used as the last option.

8.5.2 Security Aspects while Disposing

1. While disposing of an IT device or media, the Security Policy of Symbiosis shall be applied.
2. All employees are responsible for the sanitization of non-reusable electronic media before disposal.
3. The scrapped equipment should be isolated following security procedures.
4. Similar to shredding paper reports, CDs and other non-rewritable media should be destroyed before disposal.

8.5.3 Green IT Policy on Disposal

a. The obsolete items designated as scrap shall not be dumped as land-fills.
b. An authorized agent should collect scrapped material for disposal and should provide assurance that it will be disposed of by abiding the government's environment laws.

9. Policy on Internet & Social Media

9.1 Purpose

This policy describes acceptable use of Internet at Symbiosis for Websites, Email, Social Networking, Learning, and Academic Projects. It is the endeavour of Symbiosis IT services, particularly in case of use of internet, to protect the privacy and security for its users, systems, and networks.

The main purpose of this policy therefore is to provide guidelines to ensure that internet is used in a responsible manner; and information officially provided about Symbiosis on the internet in any forum is correct and up-to-date.

9.2 Applicability

1. This Policy applies to all users of internet, including students, on Symbiosis networks.
2. This policy is applicable to all Institutes and Departments or Symbiosis employees or students who represent Symbiosis on the internet through web pages, blogs and any other social media.
3. Symbiosis Network referred to in this policy represents all types of networks at Symbiosis including the local area networks at the Institutes or a Department and Symbiosis Wide area Network that may be operational.

9.3 Internet on Symbiosis Networks

1. **Bandwidth Allocation:** Symbiosis Management shall approve an appropriate bandwidth to every campus and premises based on various factors. Normally it will depend on one or more of the following:
    a. Number of users at peak time, at Institutes or departments
    b. Extent of Internet usage necessary for the curricula at the institute (Media and communication, photography etc.)
    c. Nature of academic activity carried out in the department such as research or training,

d. Use of videos/social media for academic purpose,
e. Enhanced bandwidth for event oriented requirements such as Admissions, Seminars, and Conferences.

2. While using the internet for such relevant communications it is the sole responsibility of the sender or receiver as case may be, to validate the content of the outgoing and incoming communication.
3. Any download of large or massive data files including video or audio, on Symbiosis network may be carried out only by the Network Administrators or with prior arrangement made by the Network Administrator without disturbing normal work of the Institute or Department. Such downloads may be carried out only for academic or IT administration purposes.

9.3.1 Internet Access

1. Internet access may be provided to a user with the approval of the Head of the institution
2. To maximize usage of available bandwidth for a location, judicious scheduling of the bandwidth usage should be considered. For example, use of online videos should be considered during off-peak hours or for a limited number of users during office hours.
3. Using individual network devices for disproportionate use of bandwidth, particularly in hostels, is prohibited.

9.3.2 Prohibited Uses of Internet

The following uses are prohibited under this Policy and are not intended to be exhaustive.

1. **Illegal/ Criminal Activity**
   The internet over Symbiosis Network may not be used in connection with criminal or civil violations of state, central, or international laws, regulations, or other government requirements.
2. **Improper usage of Symbiosis information on internet**
   Any addresses or data provided by Symbiosis to the users in the course of work or administration should not be published by the users anywhere on the Internet or

registered anywhere in the internet without the written permission of the Head of the concerned Institute or Department.

3. **Security Violations**

   No user of internet on Symbiosis Network shall attempt to violate the security of any other network, service, or other system whether or not successful. These include hacking of websites, illegal access to other systems or networks.

4. **Threats**

   No user of the Symbiosis Network shall transmit materials of a threatening nature of any kind on internet.

5. **Offensive Materials**

   No user of the Symbiosis Network shall use the network for the distribution of offensive materials of any kind on internet.

6. **Spam**

   No user of the Symbiosis Network shall use the network for spam including the following activities:

   i. Sending unsolicited mails that could compromise the security of Symbiosis network or provoke complaints as per the discretion of Symbiosis.
   ii. Collecting the responses from unsolicited email that could compromise the security of Symbiosis network or provoke complaints as per the discretion of Symbiosis.
   iii. Sending unsolicited email without providing a clear and easy means to unsubscribe receiving future emails from the originator of the email.

7. **Indirect Access**

   An indirect access to the Symbiosis network means, using an authorised user-id password with or without the knowledge of the authorised user. In case of any violation of this internet policy through an indirect access will be considered as the violation by the authorised user.

9.3.3 Incident Reporting & Consequences

i. Any complaint by a Symbiosis user regarding violations of this Policy should be sent to Head of the concerned Institute or Department, along with details that would assist Symbiosis in investigating and resolving the complaint. A copy of such a complaint should be mailed to chiefit@symbiosis.ac.in.
ii. Violations of this Policy may result in a disciplinary action as per Symbiosis HR policy.
iii. Symbiosis shall block a particular user-access which is provided by Symbiosis if the user is involved in any kind if ILLEGAL/ CRIMINAL activity over the Internet. Violators may also be subject to civil or criminal liability under the applicable laws.

9.4 Intranet

Symbiosis is implementing an Intranet to facilitate internal communication and access to common systems. All policies related to internet also apply to intranet. Any additional policies if required will be detailed as and when applicable.

9.5 Domain Names

1. Symbiosis IT Department shall streamline the domain names that are prevalent. It will formulate an appropriate structure for domain names, covering SIU and the Institutes & Departments under SIU, Symbiosis Society and all Institutes & Departments directly under Symbiosis Society.
2. IT department will make a transition plan for streamlining domain names.
3. Symbiosis IT Department shall assign and obtain all domain names. Institutes and Department are free to obtain sub-domains under their own domain names.
4. An Institute or Department desirous of obtaining a new domain name shall contact Symbiosis IT Department and obtain a domain name as per the policy.

9.6 Email

1. Symbiosis shall transition to two main email accounts namely for Symbiosis Society and Symbiosis International University. All existing institute email accounts shall transition to new accounts during the transition period.
2. IT Committee shall finalise Symbiosis email service provider/s whose services will be monitored by IT Department.
3. A Symbiosis email account may be opened for an authorized user who by obtaining such an account accepts Symbiosis IT Code of Conduct and agrees to abide by Symbiosis IT policy.
4. Members of Symbiosis Senior management may delegate the authority to access their email accounts to their respective executive assistants by sharing their user-id and password. In such cases the concerned executive assistant will be responsible to follow the Symbiosis IT policy. Any violation to this delegation will result in disciplinary action.
5. Group email-ids may be created for operational convenience. Similarly Function email-ids may be created for official response and action.
6. HR Department shall ensure that such an email account is inactive when an employee separates from Symbiosis.
7. Institutes shall ensure that if students are given Symbiosis email accounts their email accounts become inactive after one month of closing of their concerned programme. Closing of a programme is when official certificates of completion are distributed; for example, convocation or certificate distribution. The students must be migrated and their emails have to be retained

9.7 Website, Blog and Social Networking

1. An Institute or Department may create a website or a blog or any official presence of Symbiosis on Social Networking sites, only with the permission of the Head of the concerned Institute or Department.
2. In case a domain name is to be obtained for creating a new website it should be as per the guidelines of Symbiosis IT Policy and in consultation with the IT Department. As far as possible it must be a subdomain.
3. While creating a website or an internet presence all guidelines of applicable statutory

bodies such as UGC, AICTE etc.. should be followed. In addition, all constituent institutes of SIU shall implement all guidelines issued by SIU regarding websites and other social networking initiatives.

4. The concerned Institute or Department shall be responsible for the quality and content of the material that appears on its web site and similarly for any views and comments expressed on behalf of the Institute or Department on the social network including blogs. An Institute may constitute a committee to create and monitor contents on the web, check any malicious entry and also suggest changes or new inserts.
5. The concerned person shall ensure that correct and up-to-date information is maintained on the website or any other internet presence with the approval of the Head. This person shall also ensure timely removal of incorrect or invalid information from such sites.
6. Strict security features and access restrictions should be in place to prevent hacking or distorting of pages. Timely & frequent scrutiny of the contents should be scheduled to proactively identify any attack on the website.
7. Blog pages should be viewed to prevent any unwanted material being posted.
8. The use of social networking for political purposes is not allowed. However it may be used for business purposes related only to Symbiosis with the permission of the Head.
9. Access to such official presence should be restricted and only persons authorised by the Head shall access these sites.
10. An Institute may encourage blogging by Faculty members to interact with students. For such activities Blog sites may be created under the web site and monitored by the committee for maintaining excellence of the contents.
11. The policy allows social networking by faculty and students of an Institute. The use of social media by students or faculty members should in no way produce adverse consequences to Symbiosis as per the Internet policy of Symbiosis.

10. Policy on Procurement of IT Resources

10.1 Purpose

In the normal course, procurement of IT Resources takes place independently at Symbiosis Institutes and Departments and in some cases with the help of IT Department, largely because of autonomous nature of functioning and budgeting. As a result, a variety of IT solutions are considered for similar requirements leading to disparities in their implementation, maintenance and usefulness. For the last several years, Central Purchase and IT Purchase Committee have been engaged in reducing variety and bringing uniformity for similar requirements. This policy is in continuation of the same spirit and to bring uniformity across Symbiosis in procurement of IT resources.

10.2 Applicability

This policy is applicable to all Institutes and Departments desirous of procuring IT resources.

10.3 Planning for Procurement

1. All Institutes and Departments should make an annual IT plan for supporting enrichment of academic delivery, advancement of research or improvement in administration, and include it in the annual IT budget.
2. It is important that an Institute or Department desiring to acquire IT resources, particularly those that require large expenditure should assess its requirements thoroughly.
3. Symbiosis shall support a justified enhancement of computing capacity in terms of hardware, network, software and improving the technical aspect of the Computer Lab.
4. The Institute or Department may requisition IT resources provided it is approved in the annual budget.
5. For the purchase of an IT resource, the Institute or the Department should prepare a proposal as per the instructions of the Finance Department.
6. The proposal should include:
    a. The expected outcome of the proposed acquisition of IT resources
    b. The name of a person responsible for their implementation.
    c. Indicative prices

d. Justifications including a cost-benefit analysis and/or the intended usage of the IT resource, particularly for large expenditures.

7. Symbiosis Purchase Policies apply to all IT procurements.

10.4 Central Procurement of IT Resources

1. All IT Assets shall be procured centrally by Symbiosis Purchase department.
2. Every year rate contracts will be worked out with selected empanelled vendors for bulk purchase of IT items such as desktops, laptops, access points etc.. Such contracts will be applicable for purchases of these items by all Institutes or Departments.
3. Even for items under the central purchase contracts, Institutes or departments shall make proposals and follow purchase procedures laid down by the Finance Department.

10.5 Procurement of Other IT Resources

Procurement of IT resources that are not under central procurement contracts shall be carried out from approved vendors and as per the Purchase Policy of Symbiosis.

In case existing approved vendors cannot provide the required goods or services as per the requirements, new vendors will need to be empaneled by the IT Purchase Committee.

It will be the endeavour of Symbiosis to enlist vendors having proven track record, quality of service, technical capabilities and training where required among other criteria.

The following policies do not apply to small-value items of consumable nature or required for repairs.

10.5.1 Computing Hardware

1. For every financial year, IT Department shall identify standard configurations for commonly required computing hardware such as Desktops, Laptops, Servers etc. based on current technology trends.
2. Any Institute or Department intending to procure any computing hardware shall requisition standard configuration as far as possible. In case a different configuration is needed, it should be in consultation with IT Department.
3. Replacement of obsolete computing hardware on a large scale should be carried out in a phased manner as per the IT Obsolescence policy.

10.5.2 Networking Devices

1. Networking devices include firewalls, multiplexers, switches, routers, access points, wireless devices and any other hardware or software resource related to Networks.
2. Symbiosis intends to standardise these items across all its campuses and premises in order to ensure better efficiency, easier maintainability and easier connectivity to Symbiosis Network.
3. IT department may come up with a standard set of networking devices for every campus and premises.
4. All those Institutes or Departments which presently do not have standard network devices shall continue using the same till the time of its replacement. At the time of its replacement, a standard device should be procured.

10.5.3 Internet Bandwidth

1. Bandwidth shall be allocated to a campus or premises based on the norms approved by the management. Some of the factors used for determining norms will be the following:
    - Number of Users at the location
    - Extent of Internet usage required for the curricula delivery or academic & research activity, if academic institutes/departments are residing at the location
    - Use of videos/social media for academic purpose.
2. For event oriented requirements such as Admissions, Seminars, and Conferences additional bandwidth, if required, may be obtained on a temporary basis by the Institute directly from the provider. Additional cost, if any, for the purpose should be approved along with the proposed cost of the event. Any such additional bandwidth should not interfere with the secure network of the institute/department.
3. To arrive at the optimum bandwidth for a location, judicious scheduling of the bandwidth usage should be considered. For example, use of online videos should be considered during off-peak hours or for a limited number of users during office hours.
4. Bandwidth shall be provided to a hostel based on a standard norm for the number of residents at the hostel. Any additional bandwidth if required over and above what is provided by Symbiosis should be obtained by a student at his/her own cost.

5. A fall-back arrangement to tide over any failure of internet services may be considered to ensure continuity of critical services.
6. Selection of Internet Leased Line (ILL) Service Providers: IT Department will acquire internet bandwidth for a particular location. Normally a pair of ILL service providers shall be identified based on the feasibility, track record for reliability (Minimum interruption of service) and price. A practical mix of ILL service providers shall be identified for each location so that dependency on some specific vendors is avoided.

10.5.4 Standard Software Packages

1. Symbiosis will use licensed software packages. No pirated software should be used or loaded on individual desktops/laptops, servers or any other computing device.
2. IT Department will enter into campus agreements or other agreements for standard software packages such as operating systems, office software, endpoint security software etc.as far as possible.
3. SIU will enter into campus agreements or other agreements for software packages commonly used in the delivery of academics such as SPSS, and others.
4. Any Institute or Department intending to procure a standard software package should first check with Central IT if it is covered under a campus agreement or any other Symbiosis agreement. In case a similar but not the same package is available under such an agreement, the Institute or Department shall use the package under the agreement. Only if academic requirements demand use of software package not under any agreement, may be procured with proper justification.
5. Any software freely down loadable from the internet must be virus-free and should not have malicious content. Every software so downloaded should be protected by an up-to-date anti-virus software. Free software should not be indiscriminately downloaded to avoid any cyber threats.

10.5.5 Customised Software Application

1. Over a period of time Institutes and Departments may have developed customised IT application software either in-house or by a third party. It is the endeavour of Symbiosis, to arrive at a uniform and standard IT solutions for similar functions by

2015.

2. During this period, IT Department shall attempt to carry out usage analysis and arrive at most commonly run solutions across Symbiosis and standardise wherever applicable.
3. In case of centrally run systems such Finance or Examination etc., care shall be taken that the software solutions implemented at Institutes or Departments are compatible wherever applicable to avoid any duplication of work.
4. The ownership of all customised software shall lie with Symbiosis.

10.5.6 Website

1. Any website for Symbiosis will be created or maintained only by approved vendors of Symbiosis, if outsourced.
2. A website should be hosted in a secure environment whether on one's own server or leased from a service provider.
3. If the maintenance or content management of the website is desired to be outsourced, it should preferably be carried out by the party which developed the website. The content should be vetted by the person responsible at the Institute before final release on the website. As far as possible content-management system should be used.
4. All Websites design should adhere to Symbiosis Standards applicable to the Institute or Department in accordance with the Branding and Promotions Department and must be approved by the Head of the institute prior to publishing of the website.
5. Procurement of any software used for managing a website such as Search Engine optimisation, Content management system etc. should include providing of auditable/quantifiable evidence to show its effectiveness.

10.5.7 Other IT Resources

1. Media and other consumables, small-value spares should be considered as expenses and their usage should be controlled and monitored.
2. Peripheral devices such as printers, keyboards, mouse etc.. should be of standard makes and must be maintained regularly.
3. Projectors and teaching-aids may be procured on need-to-have basis and should go through a proper scrutiny of requirement for procurement.

4. For procurement of any other IT resource not covered in this policy IT department should be consulted.

10.6 Third Party Service Provider

In Symbiosis, IT services are obtained from third party service providers such as application software developer, AMC provider, ILL(internet leased line) service provider and others. This policy is to ensure quality of service and dependability of service providers having technical capability and sound organisation for performing all relevant contracted jobs. This policy is applicable to any Institute or Department desirous of obtaining IT services from a third party.

10.6.1 Establishing the Need

An Institute or department desirous of services from a third party shall assess the requirements by checking the following among others:

i. Thorough review of requirements and reasons why such service cannot be obtained in-house
ii. If not feasible in-house, if attempts have been made to find such services from IT Department and recommendation of IT Department
iii. Criticality of such service
iv. Provision of estimated cost in the annual budget.

10.6.2 Norms of obtaining a service

1. A third party service may be contracted from an approved vendor.
2. IT Department shall maintain an approved list of vendors for various services.
3. As far as possible an Institute or Department shall engage a vendor out of the approved vendors identified for the desired service.
4. Normal procurement procedures of Symbiosis shall be followed.

10.6.3 Procurement of Services

1. Symbiosis IT Purchase Committee shall select a vendor based on the requirements as per approved proposal.
2. The evaluation of a vendor may be carried out based on the following criteria:
    a. Technical capability required for the service

b. Market standing of the party.
c. Experience of providing satisfactory service
d. Quality of service
e. Feedback on the installed base and from clients
f. The capability for deploying support staff at Symbiosis
g. Any other criteria that establishes capability of providing service on a continued basis.

3. As far as possible any academic service desired to be obtained from a third party should be under a contract with SIU for the constituents of SIU or under a contract with Symbiosis Society for the institutes directly under the society and for any other services. For example, for training on SPSS, SAS or SAP for the constituents of SIU should be under SIU contract; for Tally package services should be under Symbiosis Society contract.
4. Librarian, Central Library of SIU, shall be responsible for procuring any database services required for academic purposes. For such services SIU will enter into contracts on campus basis and the Librarian shall monitor its usage.
5. The selected vendor shall provide Service Level Agreement (SLA) acceptable to Symbiosis.
6. The service provider shall implement and maintain appropriate safeguards for any information proprietary to Symbiosis. Any contract with the service providers must include non-disclosure clauses related to confidentiality of proprietary information of Symbiosis, valid during and after the termination of the contract.
7. Symbiosis Security Policy prevalent at the time of entering a third party contract shall be applicable to the Vendor.

11.Policy on User Accounts

11.1 Purpose

The IT resources and services of Symbiosis are provided for the advancement of academics, research, and service objectives. They are offered primarily to facilitate the academic and administrative purposes. Symbiosis intends that there should not be any access or use of IT resources and services that interferes, interrupts, or conflicts with these purposes.

This Policy provides expectations and guidelines for all users to use and manage IT resources and services at Symbiosis.

11.2 Applicability

4. This Policy applies to all stakeholders who use Symbiosis networks and IT resources for academic or administrative purposes. This policy therefore is applicable to all Institutes, Departments, employees, students, visiting faculty, guests, authorised vendors or any other person who is authorised to use Symbiosis network whether temporarily or otherwise.
5. Symbiosis Network referred to in this policy represents all types of networks at Symbiosis including the local area networks at the Institutes or a Department and Symbiosis Wide area Network that may be operational.

11.3 User Account and Access

11.3.1 User Account Creation

4. Head of an Institute or Department has the responsibility and authority to review and approve all requests to use Symbiosis IT resources, preserve, access, and disclose a user's electronic information. Head may also withdraw or restrict any of the accesses if a situation demands.
5. A System Administrator or any other technical person authorised to manage IT users, will create a user account by assigning a user-id on approval by the concerned Head. He will maintain records of approving, rejecting or modifying the request.

6. User accounts may be created in the following cases.
    a. All employees other than those in Grade IV who are required to access to Symbiosis IT facilities and services, at a level appropriate to their function and role, via a unique password protected account.
    b. All SIU students who are required to access to the Institute IT facilities and services, at a level appropriate to their enrolment, via a unique password protected account.
    c. Visiting faculty and authorised vendors may be provided with access to University IT facilities and services where the use of those facilities and services is necessary for them to undertake their role within the institute or department. Access for personnel of an authorised vendor must be authorised in accordance with procedures agreed between Symbiosis and that vendor.
    d. Guests of Symbiosis may access via a unique password protected account who are authorised on a case-by-case basis by the Head where the Guest will be visiting.
    e. Symbiosis may impose quotas on the use of IT resources and services (including print, file storage, email and internet download) and will revise them as necessary.
7. Accesses to IT resources required to carry out only the assigned functions of a user may be given. Typical accesses given to an employee who is authorised and approved by the Head are:
    a. Institute or Department Network, if applicable
    b. Symbiosis Email account, if required to communicate officially within or outside Symbiosis
    c. As per the requirements of an Application the employee is supposed to operate
    d. Any other access that is relevant to the function of the employee but that does not jeopardize the IT resources.
8. User accounts of students, faculty, visiting faculty or any other authorised user, who need to connect their personal device to Symbiosis Network, should be linked to the MAC address of their personal device.
9. Temporary user accounts may be created for use by important guests of Symbiosis on the approval of the Head. Such guest accounts should have very limited accesses and should expire within a limited number of hours.

11.3.2 Suspending & Disabling User Accounts

a. Users may have their IT access suspended immediately when there is a suspected breach of the IT policy.
b. User accounts may be disabled or limited access may be given in case of a long absence on personal grounds from Symbiosis.
c. User accounts of visiting faculty or representatives of an authorised vendor, if any, should be disabled on conclusion of their contract period that may be revived on reassignment of Symbiosis work.

11.3.3 Disabling & Deleting User Accounts

a. Users may have their IT access suspended immediately when there is a suspected breach of the IT policy.
b. When a user (not a student) no longer has a relationship with Symbiosis or is no longer authorised to have access to IT resources, the user's accounts will be disabled for a specified period, and then deleted.
c. The user accounts of all students should be closed one month after completion of their programs they are enrolled to.
d. Whenever a user separates from Symbiosis by retiring or resigning or otherwise, the System/network administrator will change his password on the last day of his association with Symbiosis to deny him/her the ongoing access.
e. HR Department will be intimated when a user account related to an employee is closed or deleted.
f. A user who has multiple relationships with Symbiosis, for instance both as a student and an employee, and who ceases only one of their relationships will have the access related to the terminating relationship removed.

11.4 Passwords

1. To prevent unauthorized access through any User's password, a password should be chosen using best practices which normally avoid using Birth dates, Names, unaltered words that could be found in a dictionary, including non-English words and words spelled backwards, telephone numbers etc.
2. Normally a password should meet the following criteria:
    a) Is between 8 and 32 characters;

b) Contains 1 numeric, at least 1 uppercase and 1 lowercase character;

c) Your password must contain any of the following special characters such as ~,!,@,#,$,%,^,&,*,(,),+,=,-,`,{,},[,],|,\,:,”,’;<>,.?,/.

3. A password should be changed regularly at most every 45 days.
4. The policy on passwords is applicable to all users.

11.5 User Responsibilities

1. All Users must fully comply with IT Code of Conduct and the standards and responsibilities of acceptable use as outlined in this policy document.
2. In particular, users must adhere to
    a. The IT Policies related to Computer Lab, Email Policy, Wireless Policy, Security Policy and Internet & Social Media Policy and applicable for using IT resources.
    b. All local, state, national, and international laws;
    c. All software license agreements acquired by the Symbiosis and SIU and their institutes and departments;
    d. All applicable policies and procedures including, but not limited to, sexual harassment, academic dishonesty.
    e. Any usage restrictions on IT resources that may be applicable from time to time.
3. Users must adhere to the following responsibilities:
    a. Self-policing of passwords and access codes;
    b. Respecting authorial integrity and the intellectual property rights of others;
    c. Respecting and protecting the integrity, availability, and security of all IT Resources;
    d. Ensuring that all data and files that the User accesses or downloads are free from any computer code, file, or program which could damage, disrupt, expose to unauthorized access, or place excessive load on any computer system, network, or other IT Resource;
    e. Maintaining confidentiality and integrity of any official Symbiosis data accessed and transmitted;
    f. Not using any IT resource for personal use or gains;

g. Reporting any security risk including, but not limited to, computer viruses, or any other “mal-ware”—that infects any IT Resource and
h. Properly backing up appropriate User systems, software, and data.