TABLE OF CONTENTS

THE INFORMATION TECHNOLOGY (IT) POLICY

1. INTRODUCTION

The Information Technology (IT) Policy of Sathyabama Institute of Science and Technology provides the procedure and guidelines that govern the responsible usage information technology resources of the Institution. Every member/user of the Institution's IT resource is expected to be familiar with and adhere to this policy, and ensure that it is used for promoting the mission of the Institution towards teaching, learning, research, and administration.

1.1 PURPOSE OF THE POLICY

- IT policy of Sathyabama Institute of Science and Technology intends to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the Institution on the campus.
- This policy provides guidelines for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the Institution.

Data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information are considered as the Information assets that are addressed by the policy.

2. SCOPE

This Policy applies to everyone who accesses Information Technology Resources, whether affiliated with the Institution or not, whether on campus or from remote locations, including students, faculty, staff, contractors, consultants, temporary employees, guests, and volunteers.

Definition of Information Technology Resources: Information Technology Resources for purposes of this Policy include,

- transmission lines, networks, wireless networks, servers, exchanges, internet connections, terminals, applications, and personal computers owned by the Institution
- resources used by the Institution under license or contract, including information recorded on all types of electronic media, computer hardware and software, paper, computer networks, and telephone systems.
- personal computers, servers, wireless networks and other devices not owned by the Institution but intentionally connected to the Institution-owned Information Technology Resources (other than temporary legitimate access via the world wide web access) while so connected.

3. USAGE:

The users shall make effective usage of campus collaboration systems, internet, wireless resources, official websites (including Institution website, conference website, journal portals, online admission systems, and course website), and Management Information Systems (MIS) and ERP solutions, Learning Management System, Remote Login based facilities of the Institution and e-Library resources.

4. PROHIBITIONS:

Any activity that will lead to the creation of a hostile academic or work environment is prohibited. The users shall not send, view or download fraudulent, harassing, obscene, threatening, or other messages or material that are a violation of applicable law or Institution policy.

4.1 Copyrights and Licenses

Users must not violate copyright law and must respect licenses to copyrighted materials. Unlawful file sharing using the Institution's information resources will be viewed as the violation of this rule.

4.2 Social Media

Users must abide by the rules of the Institution with regard to the usage of social networking sites, news rooms, chat rooms and blogs. No information shall be shared in the social media like Facebook, Instagram, Twitter etc.

unless it is approved by the appropriate authority to avoid the dissemination of unauthenticated information.

4.3 Security and Integrity

The users shall not make any unauthorised access of information in order to promote secure access of Network and Computers. The person designated as system administrator may access the information resources for a legitimate purpose.

4.4 Unified Threat management (UTM):

UTM including anti-virus, anti-spam, content filtering and web filtering shall be used for secured flow of internet and intranet based traffic in the campus to protect users from security threats. Anti-virus policy updating and security updating shall be regularly done for the protection of computing resources.

5. DATA BACKUP AND RECOVERY:

This section provides rules regarding data backup and recovery procedures, protocols, and standards. The section covers the data backup schedule, backup retention, and data recovery and outlines the minimum requirements for the creation and retention of backups. Special backup needs that exceed these minimum requirements should be implemented on an individual, as-needed basis.

- The purpose of backing up data is to store a copy of the data in the event of a disaster where data is lost or corrupt. Data recovery is the act of

restoring data from the backup in order to restore data to the desired point in time.

- Information Technology team of the Institution will be responsible for all aspects of backing up servers.
- Data maintained on Institution administrative or learning management systems, such as the Faculty Information System (FIS), Student Information System (SIS), Document Management System, and others may be permanently retained at the discretion of a department or division for such department or division's area of accountability.
- All institutional data must be copied onto a secure storage media on a regular basis (i.e., backed up), for disaster recovery and business continuity purposes.
- Organizational data is stored in an on-site and off-site location and can be easily found and recovered in the event of an equipment failure, intentional destruction of data, or disaster.
- Backups include daily incremental, weekly, and full monthly backups as defined by service or application owner. This team will also be responsible for finding and restoring data when requested or required for Disaster Recovery purposes.
- The Institution shall also periodically back up the data available on the cloud platform.

- The Institution shall make all the necessary arrangements to ensure uninterrupted power supply.

6. ASSET MANAGEMENT

6.1 Asset Management:

The Institution shall lay down business processes for the management of hardware and software assets that facilitate the usage of IT resources in the Institution. This shall include procedures for managing the purchase, deployment, maintenance, utilization, energy audit, and disposal of software and hardware applications within the Institution.

6.2 Copying and Distribution:

The Institution shall ensure that there is no violation in the copying and distribution of proprietary and licensed software. The Institution shall acquire academic license of commercial software used for academic and research purpose.

6.3 IT Accessories Replacement:

In the event of failure or malfunctioning of any of the IT accessories, requisition from the respective Departmental Head shall be forwarded to the IT Service Desk. On assessing the nature of the problem concerned, the accessory can be rectified or replaced.

6.4 IT Service Policy:

The agreement entered into by the Institution with the Service Provider shall provide guidelines with respect to its execution, delivery and performance.

7 OPERATIONAL ASPECTS

7.1Governance:

The Institution shall ensure fair implementation of this policy so as to meet its objectives. Chief Technical Officer working at the Institution Level shall coordinate various activities related to the adherence of the IT Policy in association with the IT Administrator.

7.2 Support after working hours:

The Institution should have a dedicated team to provide support during non-work time and required to be available to handle job-related activities and emergencies beyond working hours.

7.3 Individual Users:

The users are solely responsible for the activities they perform on Institution servers with their "Username / Password" pairs and IP (Internet Protocol) addresses assigned to them.

7.4 Violation of Policy:

Any violation of the basic objectives and areas mentioned under the IT Policy of the Institution shall be considered as a violation and as a misconduct and gross misconduct under Institution Rules.

7.5 Implementation of Policy:

For implementation of this policy, the Institution will decide necessary rules from time to time.

7.6 Review and Monitoring:

The Policy document needs to be reviewed at least once in two years and updated if required, so as to meet the pace of the advancements in the IT related development in the industry. Review of this policy document shall be done by a committee chaired by Vice Chancellor the Institution. The other members of the committee shall comprise of Pro Vice Chancellor, Director - Administration, Registrar and other members as nominated by the Chair.