SRI MANAKULA VINAYAGAR ENGINEERING COLLEGE

(An Autonomous Institution)

Puducherry - 605 107

IT- MAINTENANCE

Policy

Version 2.0

SRI MANAKULA VINAYAGAR ENGINEERING COLLEGE
(An Autonomous Institution)
Puducherry - 605 107

NOTIFICATION

Ref: **SMVEC / IQAC / ADMIN / JAN 2023** Date: **10-01-2023**

In the pursuance of the resolution passed by the Governing Body Meeting at its meeting held on December 31, 2022 in its resolution no. GB 2022.05.09 and the decision was taken by the Management of SMVEC

It is hereby notified for information of all concerned that the Sri Manakula Vinayagar Engineering College, Puducherry has published the policy for IT Maintenance Policy. This will come into force with immediate effect.

AA Arivalagar

Dr. AA. Arivalagar
IQAC coordinator

Dr. J. Abbas Mohaideen
Registrar

Dr.V.S.K. Venkatachalapathy
Director cum Principal

Dr. A.A. ARIVALAGAR, M.Tech., Ph.D.,
IQAC Co-ordinator
Sri Manakula Vinayagar Engineering College
(An Autonomous Institution)
Madagadipet, Puducherry-605 107.

Dr. J. ABBAS MOHAIDEEN, M.Tech., Ph.D.,
REGISTRAR
Sri Manakula Vinayagar Engineering College
(An Autonomous Institution)
Madagadipet, Puducherry-605 107.

DIRECTOR CUM PRINCIPAL
SRI MANAKULA VINAYAGAR ENGINEERING COLLEGE
(An Autonomous Institution)
Madagadipet, Puducherry-605 107.

SRI MANAKULA VINAYAGAR ENGINEERING COLLEGE
Madagadipet
Puducherry

POLICY FOR IT- MAINTENANCE OF SRI MANAKULA VINAYAGAR ENGINEERING COLLEGE, PUDUCHERRY

The IT Technical team of our institution is responsible for providing the internet facility, LAN facility, CCTVs for security and surveillance, bio-metric attendance, computers for teaching and non- teaching faculties. A System administrator and Lab in charges are appointed for the maintenance of all computer laboratories. The System administrator and Lab in charges look after daily maintenance, repairs and meet the new requirements. The annual maintenance includes all software requirements, installation, antivirus and upgradation besides maintenance of the computers, bio- metric attendance unit, and web based cameras. The electrical department of the institution performs electrical safety and its related maintenance work in the respective laboratories. All the laboratories are cleaned regularly by the House keeping employees of the institution.

PURPOSE

The purpose of this document is to create a Policy for usage, purchase, installation, maintenance and management of authorized Network devices and bandwidth in the institution. This will help in avoiding non-standardized Network devices in our campus thereby having a standard operating environment with a pre-defined Service Level Agreement.

NEED FOR IT POLICY

- IT policy is being documented for fair and transparent academic purpose for use of various IT resources in the Campus for Students, Faculty members, Management, Visitors and Research Fellowship Members.
- Institution has network connections to every computer system covering all the buildings across the campus and hostels. Also wireless connections for Student and Faculties are available. Institution is running the Firewall security, DHCP, DNS, Email, Web and Application servers and managing the network of the institute. Institution is getting its Primary Internet from BSNL with 500 Mbps bandwidth.

EMAIL POLICY

Ensures to implement that the employees use their email in a way it is aligned with the objective of the institution. Therefore, an email policy will help to ensure that employees are aware of their responsibilities when using the email, and these terms are agreed and signed. Therefore, an employee can be held accountable if there were a violation of these terms.

The institution is having own domain as smvec.ac.in. Through this, the faculty members and students can create their respective mail id and password.

PASSWORD MANAGEMENT

The following instructions are essential for a secured Password management

- Passwords belong to individuals and must never be shared with anyone else.
- Passwords should be changed every 3 to 6 months, or immediately if compromised.
- A password should be at least 8 characters long.
- Never write passwords on any paper or send through e-mail. Never include a password in a non-encrypted stored document.
- DON'T reveal or hint to anyone at your password over phone, e-mail, internet, or any form
- NEVER use the "Remember Password" feature or "Stay Signed In" feature of application programs such as Internet Explorer, Gmail, or any other program.
- NEVER use your corporate or network password (such as internet banking) on an account over the internet which does not have a secure login where the web browser address starts with https:// rather than http://
- NEVER use common words or reverse spelling of words in part of your password.
- NEVER make your password a name or something familiar, like your pet, your children, or partner. Favorite authors and foods are also guessable.
- NEVER, under any circumstances, should your password be the same as your username or your real name.
- DO NOT use words that can be associated with you such as Phone numbers, Social security numbers, or Street address.
- Do not have a password consisting of a word from a dictionary. Most basic cracking programs contain over 100000 words, and plenty of variations.

- Try to have a password with a number or mixed case letters (lowercase, uppercase, numbers, special characters). Simple substitutions like a '1' for an 'i', and '0' for an 'O' are easily guessed. Add a '%' or '$' to the middle of the password.

DATABASE POLICY

Data of the institution is centralized and maintained in common sharing in which the data can be accessed wherever necessary. An enormous storage space for storing the data is available. Student software is also utilized for storing the following MIS (Management Information System) data:

- Employee Information Management System.
- Students Information Management System.
- Financial Information Management System.
- Library Management System.
- Document Management & Information Retrieval System.

GENERAL POLICY GUIDELINES FOR DEPARTMENT, CELLS AND ADMINISTRATIVE DEPARTMENT DATA USERS:

- Data from the Institute's Database including data collected by departments or individual faculty and staff, is for internal institute purposes only.
- The role and function define the data resources that will be needed to carry out official responsibilities/rights. Through its data access policies the institute makes information and data available based on those responsibilities/rights.
- Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies, including all government agencies and surveys and other requests for data. All such requests are to be forwarded to the office.

HARDWARE INSTALLATION POLICY

In order to prevent/minimize the hardware failures the following measures are taken by the institution.

1. Warranty & Annual Maintenance Contract

Computers purchased by any Department/Cells should preferably be with 3-year on- site comprehensive warranty. After the expiry of warranty, computers would be maintained by the institution system administrator or by the external Service Engineers on call basis. Such maintenance should include OS re- installation and checking virus related problems also.

2. Network Cable Connections

All the system has been connected through the Ethernet cable ie. Twisted Pair Cable or Fiber Optic cable.

3. Software Installation and Licensing Policy

No individual is permitted to install any kind of pirated or illegal software for the existing or newly procured computer machines. Any software installation needs to be done by the system administrator after a request received from the concerned department.

4. Video Surveillance Policy

The system comprises: Fixed position cameras, Monitors, digital video recorders, Storage, Public information signs. Cameras are located at strategic points inside the campus, principally at the entrance and exit point of sites and buildings.

Signages are prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV Camera are functional and monitored.

5. Policy for Online Learning

Department requiring online meeting facility, need to send a request to the system administrator on the Online Platform well in advance to schedule the meeting and to facilitate them.

6. Website Policy

A website reflects an institution's identity and is often the first point of contact for students, faculty, researchers and others. Having the right content, language, user experience, accessibility and effectiveness for an international audience is an integral part of higher education's continuous change process. The website of the institution offers powerful opportunities for expanding its global reach and reputation. In order to have this in place a Policy for Institute website is framed.

The maintenance policy of the Institute website addresses the following:

- Thoroughly review and update the entire website (annually or after any events).
- Test the website forms/checkout process (quarterly or after any updates).
- Security updates and bug fixing (monthly or as patches are released).
- Renew the domain names (annually).
- Check backups (annually).
- Test browser compatibility (annually).
- Update dates and copyright notices (annually).
- Review contact information (annually or as needed).
- Review and update legal disclaimers (annually).

The division / department / school willing to update the contents of their page, they can send the updated contents through official email to the website maintenance team. The updates to be done will be assigned to a staff member by the Head of website maintenance team / Head of Institution. The assigned Staff member will respond to updation of webpage content requests submitted to the website maintenance team. If a request could not be processed within the stipulated timeframe, the assigned staff shall inform the sender who submitted the request/ website maintenance team / Head of Institution, Data centre about the issue/concerns.

7. IT Maintenance Procedure

- IT Problems are conditions or situations (known or unknown) that can result in an incident.
- IT Incidents are unplanned events which cause an interruption to, or a reduction in, the quality of the IT operations or services.
- Security Vulnerabilities are IT problems that present specific risks to cyber security.
- Vulnerabilities that have a high probability of being exploited and that will highly affect the Institution (risk of operation disruption, data breach, etc.) are often labeled as Critical or High.

8. SMVEC Student Software

- The Institution maintains student software. All student data including personal and academic details are maintained in this software. Faculty details, their performance details are also maintained in this software.
- When the students enrolled into the college their personal information will be loaded into this software. Daily attendance, internal mark details are updated in this software. SMS will be sent to the parents whose ward has taken leave on that day itself.
- The department and COE maintain this information. Each faculty member has been given login credentials to access this software.