10. IT-CYBER SECURITY POLICY

IT policy of St. Thomas College is aimed to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure in the campus. This policy applies to all of institution's students, faculties, administrative staff, other employees, contractors, volunteers, vendors, collaborators and anyone else who may have any type of access to institution's systems, software and hardware.

Purchase and Compliance

The Administrative department has set procedures and guidelines need to be followed to purchase new technological equipment, services or software for official purpose. All approved equipment, services and software will be purchased through the Procurement Department, unless informed/permitted otherwise, complying with government regulations.

Any employee who notices misuse or improper use of equipment or software within the organization must inform the immediate superior or the principal immediately. Inappropriate use of equipment and software by an employee will be subjected to disciplinary action as deemed fit by the Management Committee of the Institute.

Training

Basic IT training and guidance is provided to all new employees about using and maintaining their Personal Computer (PC), peripheral devices and equipment in the organization, accessing the organization network and using application software. Management will conduct IT trainings on a regular or requirement basis.

System Maintenance

Employees, who are in need of hardware/software installations or face technical issues, it shall be reported to the IT section through the online portal/means. Upon receipt of the service request, the team will respond to resolve the issue. Any questions or status checks can also be initiated using the same procedure. For tracking purposes, all supported computer/peripheral equipment must be assigned an inventory number. Technical issues will be resolved on a First-Come-First-Serve basis. However, the priority can be changed on request on the basis of the merit.

The college sets aside at least 10% of its annual procurement budgeted allocation for IT infrastructure maintenance. With this amount, it assures and provides regular maintenance and necessary upgradation. While, the college will take all reasonable precautions to keep its systems and servers in good working order, it accepts no responsibility for any loss or damage, whether direct or indirect, or for data loss resulting from its use, which rests on the users of the data.

Hardware Decommissioning Policy

- Near-obsolete devices and computers are reused internally after the typical replacement cycle of four years, for up to four more years.
- Any hard drive or other storage device in equipment being decommissioned is wiped to prevent the reading, copying, or reconstruction of the data stored, or otherwise physically destroyed to prevent the same.
- Alternatively, the hard drives or storage media must be physically destroyed so as to render any data inaccessible.
- The Service Provider must also ensure compliance with any licensing requirements in respect of the equipment.
- Measures are taken so that assets are not unnecessarily wasted or placed in the wrong hands.
- Data stored on this hardware will be preserved as needed (or securely purged), and all ancillary information regarding hardware (asset tags, location, status, etc.) will be updated.

Decommissioning Responsibilities

Hardware decommissioning (whether due to obsolescence, failure, or another reason) will be the responsibility of the Principal in consultation with Purchase Committee and IT Department. They will work with related stakeholders to make an appropriate decision as to whether or how to decommission hardware. Sometimes the decision behind whether to decommission hardware is easy-but in other cases, it can be harder to find the right answer. When in doubt, the decision should be based on the following questions:

- Is the device no longer needed?
- Is the device performing poorly and/or causing outages or service disruptions?
- Can the device be repaired/upgraded to perform more reliably?
- Is the device outdated and no longer the best choice for use?
- Is the device redundant or superseded by another one?
- What services will be affected by the removal of this device? Can they or have they been reallocated or replaced elsewhere?
- Can the device he used elsewhere (e.g., a test lab or practice system)?

With these responses, the committee can decide whether to donate, give away, recycle, or destroy the equipment. The decision will be based on the device, the personnel involved, and the security policies and procedures in place, thus it will differ from case to instance. Care must be taken to ensure that appropriate steps are taken to protect the organization, its data, and its assets.

Inventory Management

An accurate inventory of all technological assets, software and tangible equipment purchased by the organization is neatly kept. All technological assets of the organization must be physically tagged/marked with codes for identification. Periodic inventory audits will be carried out to validate the inventory and make sure all assets are up-to-date and in proper working condition as required for maximum efficiency and productivity.

Confidential Data

Some of the common examples of confidential data include:

- Student personal data
- Faculty personal data
- Classified Data pertained to Controller of Examinations
- Data about partners
- Data about vendors
- Patents, formulas or new technologies
- Classified financial information

Device Security- Using personal devices

Logging in to any of institution's accounts for personal devices such as mobile phones, tablets or laptops, can put our institution's data at risk. St. Thomas College (Autonomous), Thrissur, does not recommend accessing any institutional data from personal devices. If it is inevitable, stakeholders are obligated to keep their devices in a safe place, not exposed to anyone else.

We recommend stakeholders to follow these best practices:

- Keep all electronic devices' password secured and protected
- Logging into institution's accounts should be done only through safe networks
- Install security updates on a regular basis
- Upgrade antivirus software on a regular basis
- Don't ever leave your devices unprotected and exposed
- Lock your computers when leaving the desk

Email Security

Emails can carry scams or malevolent software (for example worms, bugs etc.). In order to avoid virus infection or data theft, our policy is always to inform stakeholders to:

- Abstain from opening attachments or clicking any links in the situations when its content is not well explained
- Make sure to always check email addresses and names of senders.
- Search for inconsistencies
- Be careful with malwares, clickbait titles (for example offering prizes, advice, etc.)
- Change all account passwords at once when a device is stolen.

In case that a student/faculty/employee/office is not sure if the email received, or any type of data is safe, they can always contact our IT specialist.

Managing Passwords

To ensure avoiding that your institution account password gets hacked, use these best practices for setting up passwords:

- At least 8 characters (must contain capital and lower-case letters, numbers and symbols)
- Do not write down password and leave it unprotected
- Do not exchange credentials when not requested or approved by supervisor
- Change passwords every 2 months

Transferring Data

Data transfer is one of the most common ways cybercrimes happen. Follow these best practices when transferring data:

- Avoid transferring personal data such as student and employee confidential data
- Adhere to personal data protection law
- Data can only be shared over institution's network

Our Network Administrators / Security Specialists should:

- Install firewalls, anti-malware software and access authentication systems.
- Arrange for security training to all faculties and students.
- Inform stakeholders regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow the provisions of this policy as other stakeholders do.

Even when working remotely, all the cyber security policies and procedures must be followed.

Disciplinary Action

We expect all our stakeholders to abide by this policy and those who cause security breaches may face disciplinary action:

Some of the examples of disciplinary actions include:

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and train the employee on security.
- Intentional, repeated or large-scale breaches (which cause any sort of damage): We will invoke more severe disciplinary action up to and including termination.
- Each case and incidence will be assessed on a case-by-case basis.
- Everyone who disregards institution's policies will face progressive discipline.