CONVENING ORDER

CYBER SAFETY CLUB 2022-23

The government of Telangana proposed to form "Safety Clubs" in the colleges of Telangana State in order to create awareness and bring ownership for various issues relating to safety among the students community. The St.Martin's Engineering College is decentralized and transparency is maintained by constituting "Safety Clubs" with students in the college. The St.Martin's Engineering College has initiated and formed Cyber Safety Club among Safety Clubs constituted with the following members:

Safety Club: Cyber Safety Club

S.No	Name of the student	Hall Ticket Number	Class & Section	Contact Number	Position
1	Monish	21K81A0526	CSE-2A	9652595873	Captain
2	HariPriya	21K81A12F1	IT-2C	8919058728	Vice-Captain
3	SriLaxmi	21K81A0420	ECE-2A	8919350910	Member
4	G.R.AntonyAkash	21K81A05F7	CSE-2C	9346115791	Member
5	B.SaiTeja	21K81A0405	ECE-2C	6305476755	Member
6	Vikas	21K81A1288	IT-2B	7731864731	Member

Faculty Co-Ordinator: Ms. K.Radha

Frequency of Meeting: Yearly Twice.

Functions and Responsibilities:

1. To educate about Dynamic Cyber security policies for students and institutes.
2 .Translate policy statements into an action plan.
3. Create awareness about risks in Cyber space.

4/1/23

PRINCIPAL

PRINCIPAL
St. MARTIN'S ENGINEERING COLLEGE
UGC - AUTONOMOUS
Survey No. 98 & 100, Dhulapally (V)
Dundigal-Gandimaisamma (M), Medchal-Malkajgiri Dt.,
Secunderabad-500 100, Telangana.

CYBER SECURITY POLICIES

I. User accounts and Administration

(a) Students and faculty should use their own accounts and maintain cyber sanitization as per Institutes instructions.
(b) Maintain required account management policies and should not tamper with their own requirements.
(c) Students should inform institutes about any type of misconfiguration found in their accounts. Teachers should also follow the same.
(c) Students should inform institutes about any type of misconfiguration found in their accounts. Teachers should also follow the same.
(d) Students and teachers should maintain their entry/exit information correctly.
(e) Students and faculty should not make any type of user account bypassing techniques and follow all rules as per IT Act 2000.
(f) Students and faculty should follow every instruction of institutes about their user account management.

II. General user accounts

(a) General purpose users should access their accounts as per instruction of faculty.
(b) Users should not try to install unwanted software/programs without prior permission of Institutes/faculty.
(c) Users should accept time to time policy implementations and follow the rules as per the guidance of faculty.
(d) Students/teachers should not use these accounts for social media/personal purposes.
(e) Students/teachers should not save unwanted images and files in this account.
(f) Students/teachers should not access other data with the help of these accounts.

III. Special user accounts

(a) Students should not access this account without prior permission of faculty.
(b) Any discrepancy in these accounts should be treated as a punishable offense.
(c) Credentials of these accounts should be kept with the lab in charge.
(d) Passwords of these accounts should be changed periodically.

IV. Physical Security

(a) Users should maintain the physical security of the system.
(b) Users and lab assistants should monitor the lab and its premises from time to time.
(c) They should make a close watching procedure on CCTV cameras and should maintain CCTV cameras in good working conditions.
(d) Lab in-Charges should ensure security management of entrance and exit of lab premises.
(e) Lab in-Charges should keep the necessary records of lab timing and asset management.

V. Password handling

(a) Password records should be maintained.
(b) Password policy should be implemented fortnightly.
(c) Passwords of each account should be kept in common records on different pages.

VI. User and access rights assignment

(a) Administrator accounts should be maintained by Institutes.
(b) Administrators should implement security policies as per requirement.
(c) Administrator should audit all computers and keep records.
(d) Access to information and information processing facilities shall be provided after due process of identification, authentication, and authorization. Access to information assets shall be controlled.
(e) The access to information and Information Systems shall be according to the principles of least privilege and "need to know basis" to authorized users.
(f) Access to information and Information systems shall be regulated using unique User IDs, Users access to information assets shall be reviewed at regular intervals. Format procedures for user access management shall be documented and communicated.

VII. Unauthorized Data

Unauthorized data like personal documents, presentations, multimedia files, etc. will not be stored within the official system or hosted on official websites.

DATA SECURITY

I. Database Administrator

A database administrator will be nominated by the institution who will be responsible for all database functions and manages the user authorized list and deals with the management of all the data stored in the database. No default roles will be commenced.

1. Data Classifications

(a) Restricted Data: Information should be classified as Restricted when the unauthorized disclosure, alteration, or destruction of that data could cause a significant level of risk to the University or its affiliates.
(b) Private Data: Data should be classified as Private when the unauthorized disclosure, alteration, or destruction of that data could result in a moderate level of risk to the University or its affiliates.
(c) Public Data: Data will be classified as Public when the unauthorized disclosure, alteration, or destruction of that data would result in little or no risk to the University and its affiliates. Examples of Public data include press releases, course information, and research publications. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

2. Multi-Level Authentication

The process ,by which more than one factor of authentication is needed to verify the identity of a client requesting access to resources. There are three common factors of authentication: something you know (e.g. password, pin, etc.), something you have (e.g. smart card, digital certificate, etc.), and something you are (e.g. fingerprint, retinal pattern, etc.). Use of single-factor authentication (username and password combination) is sufficient, even if multiple level authentications is required.

3. Failed Login attempts

Logs for all successful/failed login attempts will be maintained and reviewed regularly. Account lockout policy should be configured for locking the user account after 5 failed attempts by the user.

4. Privileged Users

Users who can alter the configuration of the system, specifically, the security configuration. This definition is intentionally vague to allow the flexibility to accommodate varying systems and authentication mechanisms. Ina traditional Microsoft Windows environment, members of the Local Administrators, Domain Administrators, and Enterprise Administrators groups would all be considered to have privileged access. In a traditional UNIX or Linux environment, users with root-level access, or the ability to do would be considered to have privileged access. In an application environment, users with 'super-user' or system administrator roles and responsibilities would be considered to have privileged access.

5. Software Configuration and Change Control

(a) All changes in hardware, software, and their configuration will be analyzed, approved, and carried out in a controlled manner under supervision.
(b) System formatting, Recovery, Repair and Restore permission from appropriate authority must be taken in prior to format, recovery, repair, or restoration of information system assets including computers and laptops, external storage disks, etc.

6. Data Security and ownership backup

Ownership of data stored within the database will rest with the database administrator and the security of the data will be ensured by the database administrator. There may be instances where the application is able to generate information of much higher significance than the information fed to the database. Responsibility for the security of any such information prepared by collating base data will be of the authorized user who is authorized to access the collated/aggregated information. Backup of data will be taken and tested regularly as per the backup policy of the establishment and criticality of the information.

II. Network and Communication Security

Rules to access both internal and external network servers/resources:
(a) Use of network services and its resources will be formulated by the head of the Cyber team and national IT security policy. The policy clears the methodology that users must follow to access authorized networks and resources.
(b) Equipment like network devices and terminals will be configured to automatically identify the device on a network. Devices must confirm its identity to complete the handshake with network devices.
(c) Usage of third-party applications for remote access on a network, like zoom meetings, Teams, Webex, and VNC should be avoided on official networks.
d) Routing restrictions must follow within the network connections to secure the valuable information of the college/university.
(e) Device management on a network like a switch, Medium Access Control MAC, and IP

binding must be implemented and minimize the usage of ports within the network switches deployed over a network.

1. Remote access to a network

Remote access to the sources on the LAN side of the network of any institution will only be permitted for pre-designed and authorized users only. The privileges granted for remote access need to be restricted. Permission for such remote access, if required, will be given by specified authorities.

2. File Transfer Protocol (FTP)

Users of insecure FTP services are not recommended. However, the use of secure FTP services may be configured using network technologies like secure socket layer/transport layer security (SSL/TLS) protocols.

3. Mobile Phone Usage

(a) Mobile /Smart Phones and smart watches /wearable devices with data connectivity are prone to be exploited for siphoning of information of remote locations/ servers without the knowledge of the user. Moreover, mobile phones with GPS facilities can be tracked in real time without the knowledge of the user.

(b) The risk posed by mobile phones is proportional to the various advanced features integrated within the device. Inbuilt features like camera, data storage capability (fixed and removable), Bluetooth, NFC, infrared port, Wi-Fi, and GPS cannot be completely disabled and pose a threat to data and location security.

III. Security Zone Assignment

1. Hardware and Software Asset Protection and Management

(a) Hardware Protection and Management:

(i) Management of IT Assets: Glossary of IT hardware and peripherals will be managed and protected by Cyber security officers and Network Administrators who are appointed and elected by governing bodies of a college or university at all levels. Usage and Accountability of IT assets, logbooks will be maintained by college

(ii) Data drain and destruction: Damaged optical media, tapes, hard disks System logs, printouts, printer ribbons, printer cartridges should be destroyed in a secure manner. Records will be kept for the equipment by the college/university.

(iii) Backup of Important Information/Data: Secure data, data backup, and the system should be taken timely. Backup data to be stored in a fire and waterproof container or a safe and safeguard against natural disasters.

2. Software Protection and Management

(i) Only licensed versions of OS (Windows/ Linux application) and custom software (MS Office, Adobe) should be used. Users should not install any OS other than provided by the Administrator and the administrator ensures the hardening of computers and servers. Dual boot and virtualized OS installation are strictly prohibited.

(ii) Application software should be licensed and should be periodically checked by the administrator and issuing authority.

(iii) Software patch management of OS, security software, applications, web browsers, is one of the best protection methods against malware and other online threats. User/system administrators should check periodically whether all software's are regularly updated with genuine patches.

(iv) Pirated Software: Since pirated software is embedded with malicious codes and cannot be updated, the use of pirated unlicensed /cracked software is strictly prohibited within the official system.

3. Server Room Protection

(a) Multi-level authentication including biometric authentication to restrict access by unauthorized personnel. Two-factor authentication is required for PCs handling important data.

(b) Features like camera Wi-Fi, voice recording, Bluetooth, GPS, and geotagging must be disabled on all official devices like computers, Laptops, and Tablets. Cordless mouse, Keyboard, and presenters are, however, allowed to be used.

4. Power Damage Prevention

Power loss can lead to vital data loss and in some cases, it may even lead to system crash/failure. So, IT equipment should be protected from power failures and other disruptions. Standby arrangements, in terms of uninterrupted power supply and backup power, shall be used.

5. Storage Media strict control is required to be exercised in the use of mass storage devices such as CD/DVD writers and Ethernet-based hard drives/ Network Attached Storage (NAS) Drives. Explicit authority to specified persons must be issued for usage of these devices and a periodic check of accounting procedure should be undertaken. Cyber security audits must ensure a comprehensive check of all related security aspects.

IV. Security Audit And Incident Handling

1. Security Audit:

(a) Cyber Security Audits will be forced at all educational institutions to ensure and follow cyber security policies and advisories issued by AICTE and National IT security policy. AICTE nominated a Chief Security Audit Officer (CSAO) and a team of members to conduct an audit periodically as per the advisory.

(b) Audit will be conducted by institutions, colleges/universities four times in a year. Chief Security Audit Officer (CSAO) is responsible for periodically reviewing/arranging to review the levels of information and cyber security and its implementation across colleges /universities and institutions. The internal audit team may obtain the necessary support from the Information Security Team to carry out the audit work.

2. How to Manage the Response to an Information Security Incident

To ensure effective management of information and cyber security incidents, including responding to a cyber crisis, and preservation of digital evidence.

(a) A formal information and cyber incident management shall be established to discover, record, respond to escalate and prevent information security events and weakness effectively

(b) A Cyber Security Cell shall be established to monitor the critical IT infrastructure and information systems of institutions to provide analysis, intelligence, and response for different information and cyber security threats to the latest projects and classified documents of institutions. Monitoring of threats shall also consider threat intelligence and advisories.

(c) All users of information systems including suppliers shall report any security breach or attempt to breach and security weakness in information systems to a designated authority.

(d) Cyber crisis Management Plan shall be designated and implemented for an effective response to cyber crisis incidents. Only Authorized officials shall report information on cyber security incidents to outside authorities when such reporting is required to comply with legal, statutory, regulatory requirements.

3. Breach of Physical Security

(a) Access security such as access cards, biometric access devices, controlled entry points, and manned reception will be used to establish secure entry.

(b) Protection from environmental threats: precautions against fire accidents, lightning, and all other types of natural or man-made disasters will be taken; all data processing facilities and complexes shall be equipped with proper firefighting systems, automatic smoke detectors, and temperature monitoring sensors to prevent

Dos and Don'ts

(a) A genuine operating system is recommended with regular updates.

(b) Latest updated version of antivirus aids in protecting the computer from Cyber-threats.

(c) A personal computer needs to have good malware, anti-spyware. The recommended downloads are Malware byte, Super Antispyware, and useful cleaners.

(d) Use strong power on password, Admin password, and user login password. An alphanumeric password with special characters will be helpful. Changing them regularly minimizes the risk of Cyber-threats.

(e) Never click on attachments of email that you are not sure of. Think before you click.

(f) Work on sandbox which is an important security technique that isolates programs, preventing malicious or malfunctioning programs from damaging or snooping on the rest of your computer.

(g) Always backup your data on an external Hard Disk Drive.

(h) Format your personal computer regularly.

(i) Always save the passwords in a coded format.

(j) Use secure erase software for deleting files.

(k) Do not access, store, share, and manipulate official data on the personal computer.

(l) Firewall or IP Tables must be configured on every system and kept on at all times.

Guidelines for the operating system used on residential internet computer (Window or Linux)

(i) Keep Wife /Bluetooth service disabled (when not in use)

(ii) Disable all default and manual shared drives and folders.

(iii) Provide minimum rights to the user account.

(iv) Enable security features of windows like firewall, security policies.

(v) Disable Guest account.

(m) Do not download any unwanted software, clear scrutiny is recommended before any download.

(n) To safeguard against fake/malicious applications/software used to compromise and extract information from the internet computers, all software/ applications like browsers, antivirus software, etc to be downloaded directly from OEM (Original Equipment Manu-facturers) website or a licensed version of the same be procured.

(o) Configure your modem and Wi-Fi devices. Always change the default password.

(p) Smart phones are also vulnerable to cyber-threats and must be configured for their secure use.

(q) Change your email password regularly.

(r) Use secure browsers like updated versions of Chrome and Firefox for surfing. Configure web browser as

Under:-

(i) Disable window pop-up functionality.

(ii)Disable Java runtime support.

(iii)Disable ActiveX Support.

(iv)Disable all multimedia and auto-play/auto-execute extensions.

(v) Prevent the storage of non-secure cookies.

(vi) Ensure that the downloads cannot be automatically run from the browser.

(u) Most of the Smart phones allow for locking the screen by means of a security PIN. This is a good practice for preventing unauthorized access to the device if left unattended or lost.

(v) Data, if stored on the device must be encrypted.

(w) Do-not install untrusted applications. Always check for the permissions requested by the application. Do not install the application if suspicious permissions are requested by it.

(x) Install an updated internet protection suite (a combination of antivirus and firewall).

(y) Sanities all data by carrying out a virus scan before it is downloaded.

(z) Do-not turn on geo tagging and location service. It is strongly suggested to minimize the use of Location

Service.

(i) Do not click on a link /photo sent by a stranger.

(ii) Do not use unknown Wi-Fi in public places like airports, railway stations, bus stops, shopping complexes, etc.

(iii) Old smart phones are to be disposed of in a secure manner.

(iv) Do not make smart phone devices as storage for personal data.

(v) Note down the IMEI (International Mobile Equipment Identity) number of the smart phone in a safe location.

(vi) It is a good practice to use cloud storage for backup of the smart phones and systems in a secure manner.

(vii) Trusted gaming sources ensure network security and control.

(viii) Emails from an unknown source or originator to be ignored or authentically confirmed before accessing.

(ix) Report any suspected E-mails/ Messages and Pop-ups.