



Mahavir Education Trust's

SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE

Affiliated to University of Mumbai & Approved by DTE & AICTE
UG Programs accredited by NBA for 3 years w.e.f. 1st July, 2019

SAKEC

Cyber Security Strategy

&

Cyber Incident Response

Policy



W. T. Patil Marg,
Mahavir Education Trust Chowk,
Chembur, Mumbai - 400 088.



+91-22-25580854
+91-22-67978100



Email : info@sakec.ac.in
www.shahandanchor.com

SAKEC Cyber Security Strategy & Cyber Incident Response Policy

Overview

Internet connectivity presents us with new dangers that must be accounted for to safeguard our infrastructure, people and vital information assets. Access to the internet is provided to all faculties, staff and students. Higher education institutions hold vast amounts of data and are constantly subjected to cyber attacks, including personal information about students, faculty, and staff, intellectual property, research data, innovation data, and donor information, making them attractive targets for hackers.

The College's specialized assets – including but not limited to desktop, laptops, servers and portable computer systems, fax machines, VOIP systems, electronic mail (email), electronic announcement sheets, and its intranet – are essential and vital pieces to its operations. Since these challenges and threats are rapidly evolving it's more efficient to design and explain the role of the college.

Vision :

A safe digital environment can advance its economic prosperity and national security by providing innovative cybersecurity education, training, and awareness at the institute level. The institute is at risk of cyber attacks, forcing it to design and implement procedures to protect valuable information.

Mission:

To make SAKEC one of the most favoured IT enabled Institutions by combining strategic planning with the development of a globally competitive and sustainable IT Resource Campus.

Goals:

- Create a dynamic well-fitted cyber security policy for the institute.
- To establish a documented approach to information security.



- Translate policy statements into actionable plans.

Purpose and Scope of the document

- This policy document explains the rules for how employees, students, faculties and other staff members access the internet and its resources and applications while transmitting data across the internet while maintaining sufficient security.
- The objective of this policy is to define the best utilization of the internet by the students, faculties and staff of the Shah and Anchor Kutchhi Engineering College (SAKEC).
- Effective policies are often necessary in the event of an IT audit or litigation, in the form of sufficient data and proper safety mechanisms to stop malicious actors.
- This policy establishes Campus-wide rules and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the management.
- This policy is applicable to all internet users (Faculty, Technical staff, Administrative staff, Contract/Temporary staff and Students (BE/ME) who access the internet provided by the SAKEC through any and all means. All users utilizing the institutes IT resources should operate within the bounds of this policy.

Internet Access Usage

- Users not conforming to these policies will be subject to disciplinary actions. Internet access will be discontinued upon completion of study of students, completion of contract, transfer of faculty/staff, or any disciplinary action arising from violation of this policy.
- The privileges granted to users are being rigorously monitored and may be revoked at any time if it is no longer needed by the user or by decision of management if deemed to be in violation of this policy.
- Internet users of SAKEC shall comply with applicable National/State/Cyber laws and rules and policies of the management. Examples of Rules and policies include, the laws of



privacy, copy right, trade mark, obscenity and pornography. The IT act 2000 which prohibits hacking, cracking, spoofing and similar activities.

- According to the management IT policy, the tethering/hotspotting of internet connection is liable for deactivating the connection. Users will be required to obtain necessary authorisation before using college connectivity.

User Accounts and Administration:

- Students and faculties should use their own accounts and maintain cyber sanitization as per institutes instructions.
- Students must inform the institute about account compromises or irregularities.
- Students and other institute members should not carry out any actions which puts them in violation of "IT Act 2000".

Student Accounts:

- Students should access the account as per the instructions laid out by the institute.
- Students should not install unwanted/unnecessary softwares without prior permission of faculty.
- Students should not use their accounts for personal purposes.
- Students should not save unwanted information in this account.

Staff Accounts:

- Staff should access the account as per the instructions specified by the institute.
- Staff should not use accounts for their personal purposes.
- Staff should not use social media for personal purposes.
- Staff should not install any software without seeking permission from the IT team.



Physical Security:

- Users and Lab assistants should monitor the labs always.
- Lab in charge should make necessary records of asset management.

Data Security/System Analyst:

A database administrator will be nominated by the institution HE/SHE will be responsible for all database functions and manages the user authorized list and deals with the security management of all the data stored in the database.

Data Classification:

- Public Data : An unauthorized access of this data could result in no risk to an institute.
- Restricted Data : An unauthorized access of this data could result in significant risk.

Software Configuration and Change Control:

Any changes in software, hardware and networking devices will be analyzed and approved in a controlled manner under supervision with prior permission.

Network and Communication Security:

- Rules to access both internal and external network resources.
- Remote access to the resources outside the network will only be permitted for authorized users only.
- FTP Services can be configured only through SSL/TLS protocols.

IT Audit and Incident Handling:

IT Audit will be conducted by the institute at frequent intervals to ensure the proper procedure is being followed. The internal audit team may obtain the necessary support from the IT department to carry out the necessary work.



The incident response team is responsible to investigate and analyze the incident and its impact on the institute. The team should also perform immediate recovery strategies. They should always be in communication with upper management.

Roles and Responsibilities:

1.Management : The role of management is to provide all the necessary support in terms of finance and resources.

2.Principal: He/she will be responsible for taking important decisions and allocating funds for secured premises.

3.Staff: All staff members should be responsible for following the IT policies specified by the institute and guiding the students to make understand the importance of following organization IT policies.

4.Students: All students will be responsible for following the IT policy guidelines and inform the staff in case of any compromises or attacks on accounts.

Each user is responsible for the content of all text, audio, or images that they place or send over the College's technical resources. Staff may not access any data that they do not have an explicit need to or proper permissions to.

Violations of any guidelines and rules set in this policy will result in disciplinary action up to and including expulsion. In addition, the College may advise appropriate legal officials of any illegal violations and cooperate in investigations conducted by legal officials.

Use of institute internet is not permitted for the following cases:

- Operation of a business or other commercial use
- Solicitation for personal gain
- Sending chain letters or spamming
- Gambling
- Downloading Movies and games.

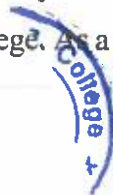


- Viewing movies and playing games
- Accessing stockbroking sites and dealings with Stock Market
- Malicious actions, such as denial of service attacks
- Harassment of other computer users
- Accessing and/or distribution of pornographic materials
- Copyright violations
- Offering of network or Internet access services
- Bit-torrents, File-sharing or other bandwidth intensive applications that may degrade quality of service
- Wireless spectrum interference or disruption of other authorized communications
- Engaging in any other activity in violation of local or state or central law

The unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material on the Internet is expressly prohibited. To ensure a virus-free environment, only the IT department is authorized to download/install files and software from the Internet onto college-owned devices.

Usage Policy of email account with “sakec.ac.in” as top level domain :

- Users will also be responsible for any activity originating from their account. In case of unauthorized use of an account, detected or suspected, the account owner should change the password and report the incident to the Principal immediately.
- Users shall not use college network and connectivity to get unauthorised access to remote computers.
- The College asks you to keep in mind that when you are using the College’s computer you are creating College documents using a College asset. The College respects the individual privacy of its staff. However, that privacy does not extend to a staff’s conduct or to the use of College-provided technical resources or supplies.
- The College’s computer, voicemail, e-mail, or telephone systems, and the data stored on them are and remain at all times the property of the College. As a result, computer data, voicemail



messages, e-mail messages, and other data are readily available to numerous persons. If, during the course of your employment, you perform or transmit work on the College's computer system and other technical resources, your work may be subject to the investigation, search, and review of others in accordance with this policy.

- All information, including e-mail messages and files, that are created, sent, or retrieved over the College's technical resources is the property of the College, and should not be considered private or confidential. Staff have no right to privacy as to any information or file transmitted or stored through the College's computer, voicemail, e-mail, or telephone systems. Any electronically stored information that you create, send to, or receive from others may be retrieved and reviewed when doing so serves the legitimate educational interests and obligations of the College. Staff should also be aware that, even when a file or message is erased or a visit to an Internet or Web site is closed, it is still possible to recreate the message or locate the Web site.
- The College reserves the right to monitor your use of its technical resources at any time. All information including text and images may be disclosed to law enforcement or to other third parties without prior consent of the sender or the receiver.

Security and Privacy

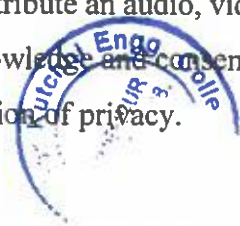
- Users should engage in safe computing practices by establishing appropriate access restrictions for their account and computing devices, guarding their password and changing them regularly.
- Users should note that their uses of College connectivity are not completely private. As part of the security measures, all the activities are logged and monitored. The College, in its discretion may disclose the results of any such general or individual monitoring including the contents and records of communication to the appropriate authorities or law enforcement agencies and may use those results for disciplinary procedures.

Prohibited Downloads



The following downloads are specifically not allowed on computers unless approved. Theft or other abuse of the campus network, computers, or computer time, including but not limited to:

- Unauthorized entry into a file to use, read, or change the contents or for any other purpose.
- Unauthorized transfer of a file.
- Unauthorized use of another individual's identification or password.
- Use of computers or computing facilities and resources to interfere with the work of another student, faculty member, or University official.
- Use of computing facilities and resources in violation of copyright laws.
- Illegal Use: Transmission, distribution, or storage of any material in violation of an applicable law or regulation is prohibited. This includes, without limitation, pornography, viruses, worms, or harmful code, material protected by copyright, trademark, trade secret, or other intellectual property right used without proper authorization.
- Threats: Threats of bodily harm or destruction of property, or any other communication that constitutes an illegal threat or harassment.
- Reselling: The resale of Internet Service or otherwise making available to anyone outside the premises the ability to use the Service (i.e. Wi-Fi, or other methods of networking) without proper authorization.
- Impersonation/Forgery: The use of the Internet Service for the impersonation of another person for any purpose, including, without limitation, adding, removing, or modifying email or network header information, use of free email services, selling or auction services, and chat or other instant messaging services.
- Email: Sending unsolicited mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material ("email spam"). This includes, without limitation, bulk-mailing of commercial advertising, informational announcements, and political tracts.
- Use of any technology to create, display or distribute an audio, video, digital file, picture or film of another individual without that person's knowledge and consent while the person is in a place the individual would have reasonable expectation of privacy.



- Any peer to peer file sharing application: Such applications may be used to utilize bandwidth inappropriately. Further, these applications contain third-party applications called adware or spyware, that collect information about a user's Web surfing habits, change system settings, or place unwanted advertising on the local computer. So users should thus refrain from such activities.
- Any third party personal antivirus or firewall: Since adequate security has already been provided for all machines via predefined firewall rules, third party firewalls may interfere with these rules thus endangering the network.
- Any Proxy servers, private fire wall, tunnelling software, connectivity sharing software
- Hacking tools of any sort: The use of any such tools on college networks is strictly prohibited. Games & Movie trailers or previews.
- Any other copyrighted content/materials/software which are not appropriate to the user or institute

Enforcement

- Users found violating this policy will be subject to penalties and/or disciplinary action.
- The SAKEC network admin may suspend, block or restrict the access to an account, when it reasonably appears necessary to do so in order to protect the security, integrity or functionality of the network.
- Suspected violations of applicable laws will be referred to appropriate law enforcement agencies.

Incident Reporting Process:



In case of any incident send description of incident or screenshot to SAKEC CYBER INCIDENT RESPONSE PORTAL

Purpose of Incident Response Policy

This document allots and describes the responsibilities of all SAKEC members for responding and reporting information security incidents.

Applicability

This policy applicable to all doing any operation of data in all three states across SAKEC IT infrastructure. That person can be a SAKEC employee, student, temporary worker, contractor, and everyone who is authorized to access the SAKECs information technology assets.

Definitions

- **Event:** A security event is described as the occurrence or change of a particular set of circumstances. Events can have a positive or negative cause. When something happens it's an event.
- **Incident:** An incident can be anything along the lines of unauthorized access, destruction of information, data breach, computer system breach, etc.
- **Information security:** Preservation of confidentiality, integrity, and availability of information.
- **information security incident:** Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
- **Incident response:** It is a set of information security policies and procedures that you can use to limit or transfer risk in case of a breach.

Policy Statement:

1. All the members of the SAKEC must responsibly report any suspected or confirmed data breaches or any kind of security incident that involves SAKEC data, the incident must be reported in brief to the responsible team.
2. All members must cooperate with the team which is responsible for handling the incident, no individual must interfere, obstruct, or prevent the smooth flow of incident response investigations.



3. During the incident investigation the responsible team is authorized to retrieve any communications or any other relevant records which are related to the incident without any notice or approval in accordance with SAKEC cybersecurity policy.
4. All the members of SAKEC should regularly participate in training, awareness, and exercise incident response to strengthen the SAKEC's ability to handle incidents when least expected.
5. SAKEC must make sure that drills and regular trainings of how to handle data breaches and ensure best security policies, must be carried out regularly and properly announced to all relevant members of SAKEC.
6. Failure to adhere to policies will be met with disciplinary actions.

Disclaimer

- The management reserves the right, without notice, to limit or restrict any individual's use and to inspect, copy, remove or otherwise alter any data, file or system which may undermine the authorized use of any computing facility or which is used in violation of rules and policies.
- Institute management reserves the right to inspect any and all resources comprising but not limited to SAKEC student accounts to inspect for any violation of IT policy or misuse.
- SAKEC has no responsibility for loss of data or inference with files resulting from its effort to maintain security and privacy or carry out maintenance.
- The management reserves the right to amend these policies at any time without prior notice and to take necessary actions to comply with applicable laws.




Dr. Bhavesh Patel
Principal