MAHARASHTRA SHIKSHAN PRASARAK MANDAL'S, CHANDRAPUR 4793

SOMAYYA

INSTITUTE OF TECHNOLOGY

Approved by AICTE New Delhi, DTE Mumbai, Govt. of Maharashtra
& Affiliated to DBATU

DTE Code 04703

SIT/committee/2024/39-(K)

Date - 2/12/2024

Measures for Cyber security The Document for Cyber security Strategy and Incident Response Policy

Following cyber security measures are implemented at Gateway Level at Institute premises:

- Firewall
- VLAN
- Access Control List- Protect access with efficient identity management
- Security roles and responsibilities
- Policies for Internet and social media usage
- Intrusion Detection System
- Network Monitoring System
- Content/Web filtering system
- Internet security/Antivirus programs on each computer
- Backup sensitive data on external storage media
- Update programs and systems regularly
- Raise cyber security awareness

1. Vision

A secure digital environment can advance its economic prosperity and national security through innovative cyber security education, training, and awareness at institute level that addresses the full spectrum of cyber security. The Institute possess massive amounts of data that includes personal information about students, faculty, staff, intellectual property, research data and innovation data due to which the institute is at a risk of cyber attack which forces to design and implement the security policies and procedures to protect the valuable information and maintain secure environment.

2. Mission

To enhance the overall cyber security framework of the institute by providing the best strategy of Cyber security.

3. Goals

Create Dynamic Cyber security policies for students and institute r Raise awareness about risks in Cyberspace . Provide guidance for the protection of critical data, IT assets and infrastructure at the Institute level

Section 1:

Create Dynamic Cyber security Policies for Students and Institute User qccounts ?nd Administmtion

(a) Students and faculty should use their own accounts and maintain cyber sanitization as per Institute's 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.

(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 the institute about their user account management.

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. User and Access

Rights Assignment

(a) Administrator accounts should be maintained by Institute.

(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) Access to information and Information systems shall be regulated using unique User IDs. Data Security Database Administration 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.

Data Classifications

(a) Restricted Data: An unauthorized disclosure, alteration, or destruction of that data could cause a significant level of risk to the Institute

(b) Private Data: An unauthorized disclosure, alteration, or destruction of that data could result in a moderate level of risk to the institute.

(c) Public Data: An unauthorized disclosure, alteration, or destruction of that data would result in liule or no risk to the Institute.

Roles and responsibilities

1.1 Role of the Board / Management:

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

1.2 Role of the Director:

Director will be responsible for taking important decisions and allocating funds for secured premises.

1.3 Role of Staff:

All staff members should be responsible for following the IT policies specified by institute and guiding the students to make. Understand the importance of following organizational IT policies.

1.4 Role of Students:

All the students will be responsible for following the IT policy guidelines and inform the staff in case of any compromises or attacks on accounts. Policy Compliance I Compliance Measurement The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner. 2 Exceptions Any exception to the policy must be approved by the In fosses team in advance. 3 Non-Compliance An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Measures for Cyber security Committee

As per the AICTE guideline the Measure for Cybersecurity Cell Following members are constituted for the academic year 2024-25. All committee members ar5e here by requested to adhere to norms of State or Central Government.

Sr. No	Name	Designation	Contact No.	Email ID
1	Dr. P. A. Gadge	Chair-person	9284769238	padmanabh06@gmail.com
2	Prof. K. D. Kadukar	Member	9960981138	kalyanidattakadu210@gmail.com
3	Prof. N. Y. Ganvir	Member	9112690494	nareshganvir2018@gmail.com
4	Prof. S. S.Bobade	Member	9399875571	sulbha.bhogale@gmail.com
5	Prof M T Sheikh	Member	8698709070	tahirsheikh@gmail.com

Somayya Institute of Technology
Seal
Chandrapur

Principal
Dr. P. A. Gadge

Principal
Somayya Institute of Technology
Chandrapur