The Shirpur Education Society's
R. C. Patel Institute of Technology, Shirpur

Measures for Cybersecurity

The Document for Cybersecurity Strategy and Incident Response Policy

Table of Content

1. Vision

A secure digital environment can advance its economic prosperity and national security through innovative cybersecurity education, training, and awareness at institute level that addresses the full spectrum of cybersecurity. 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.

Mission

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

Goals

- Create Dynamic Cybersecurity policies for students and institute
- 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 Cybersecurity Policies for Students and Institute

User accounts and Administration

(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.

Academic Policy and Strategy of Cybersecurity and Management

General User Accounts:

(a) General purpose users should access their accounts as per instruction of Institute/faculty.

(b) Users should not try to install unwanted software/programs without prior permission of Institute/faculty.

(c) Users should accept time to time policy implementations and follow the rules as per the guidance of Institute/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.

Special User Accounts

(a) Students should not access this account without prior permission of Institute/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.

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 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.

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 little or no risk to the Institute.

Software Configuration and Change Control

(a) All changes in hardware, software, and their configuration will be analysed, 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.

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 Institute/faculty. 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.

(c) Remote access to the sources on the LAN will only be permitted to authorized users only.

Security Zone Assignment

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 Institute/faculty &/ Network Administrator. Usage and Accountability of IT assets, logbooks will be maintained by institute.

(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.

(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.

(b) 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.

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

(iii) User/system administrators should check periodically whether all softwares are regularly updated with genuine patches.

(iv) Use of pirated unlicensed /cracked software is strictly prohibited within the official system.

(c) Server Room Protection

(a) Multi-level authentication including biometric authentication to restrict access by unauthorized personnel.

(d) Power Damage Prevention

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.

Incident Handling

How to Manage the Response to an Information Security Incident

(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) 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.

(c) 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.

Section 2: Translate Policy Statements into Action

Threats

A large variety of cyber threats, aimed at obtaining confidential information, pose great threats to data users. Information Security Officers are responsible for protecting, securing, and storing data, including financial aid applications, sensitive research information, intellectual property, information within online learning portals, operational data, and more.

(a) Denial of Service (DoS): During the DoS attacks, individuals who are normally granted access to systems or networks are suddenly denied the ability to view data or systems. This can include emails, Websites, learning accounts, etc.

(b) Malware: When an unrequested software is installed on an individual's computer or on a server; its access(unauthorized) will be restricted causing a system crash, it can be considered malware.

(c) Phishing: Phishing victims are targeted via unscrupulous email messages that hyperlink to fraudulent Websites via which users are prompted to disclose information such as addresses, usernames, and passwords. Implementing cybersecurity training and emphasizing individual preparedness are the best defence against phishing attacks.

(d) Ransomware: Ransomware blocks access to a victim's data, typically threatening to delete it if a ransom is paid. There is no guarantee that paying a ransom will regain access to the data. Ransomware is often carried out via a Trojan delivering a payload disguised as a legitimate file.

(e) SQL Injection: SQL injection is a kind of attack that employs malicious code to manipulate backend databases to access information that was not intended for display. This may include numerous items including private customer details, user lists, or sensitive company data.

(f) Password Attack: A password attack simply means an attempt to decrypt or obtain a user's password with illegal intentions. Crackers can use password sniffers, dictionary attacks, and cracking programs in password attacks. There are few defence mechanisms against password attacks, but usually, the remedy is inculcating a password policy that includes a minimum length, frequent changes, and unrecognizable words.

(g) Eavesdropping Attack: Eavesdropping attacks start with the interception of network traffic. An Eavesdropping breach, also known as snooping or sniffing, is a network security attack where an individual tries to steal the information that smartphones, computers and other digital devices send or receive. This hack capitalizes on unsecured network transmissions to access the data being transmitted. One way to protect against these attacks is knowing what devices are connected to a particular network and what software is run on these devices.

(h) Brute-Force and Dictionary Network Attacks

Dictionary and brute-force attacks are networking attacks whereby the attacker attempts to log into a user's account by systematically checking and trying all possible passwords until finding the correct one.

Insider Threats:

Not every network attack is performed by someone outside an organization.

Inside attacks are malicious attacks performed on a computer system or network by an individual authorized to access the system. Insiders that carry out these attacks have the edge over external attackers since they have authorized system access. They may also understand the system policies and network architecture.

Insider threats can affect all elements of computer security and range from injecting Trojan viruses to stealing sensitive data from a network or system. The attackers may also affect the system availability by overloading the network or computer processing capacity or computer storage, resulting in system crashes.

Man-in-the-Middle (MITM) Attacks:

Man-in-the-middle (MITM) attacks are a type of cybersecurity breach that allows an attacker to eavesdrop a communication between two entities. The attack occurs between two legitimate communicating parties, enabling the attacker to intercept communication they should otherwise not be able to access.

AI-Powered Attacks:

AI can be used to hack into many systems including autonomous vehicles and drones, converting them into potential weapons. AI makes cyber-attacks such as identity theft, password cracking, and denial-of-service attacks, automated, more powerful, and efficient. It can also be used to kill or injure people, steal money, or cause emotional harm. Larger attacks can as well be used to affect national security, shut down hospitals, and cut power supplies to entire regions.

When facing cyber threats, cybersecurity mitigation and response teams identify risks and cyber threat areas; protect and implement safeguards; detect cybersecurity threats; respond to a potential incident or threat; and recover and restore capabilities.

Preparing for Threats:

Preparing for cyber threats involves the implementation of a variety of prevention, protection, and mitigation strategies for use by students, faculty and staff. It is a continuous process that requires cyber security staff, and emergency management teams to constantly monitor new and emerging technologies, trends, and Information security techniques. The following are some steps that are taken to prepare for cyber threats that may impact institutes networks and systems.

Securely store data: A major element of secure data storage involves the performance of regular data backups. Even if a cyber attacker is successful in retrieving data, data backups can help cybersecurity teams "go back in time" in order to help confirm which systems, applications, etc. were compromised, which will in turn help administrative staff communicate pertinent information to those affected.

Create access control lists and firewalls: Controlling access is a great mitigation technique to use in the open environment on campuses. Accessing control lists and firewalls make it easier for IT and cybersecurity staff when they are providing user and/or investigative support before, during, and after a data breach. It is recommended that lists are reviewed on a regular basis to ensure they do not include staff who have transitioned out of positions and to add new staff joining.

Develop policies on secure deployment, maintenance and responsible/acceptance: There are a lot of players in cybersecurity prevention, protection, and mitigation. They include IT staff, emergency management teams, cybersecurity professionals, as well as faculty, students, and visitors. Policies that clearly outline what to do and what not to do when performing specific actions can help prevent cyber-attacks. Furthermore, it is recommended that existing faculty, students, and visitors receive regular notifications and reminders related to responsible cyber use and that responsible use policy are shared in the orientation packets of new faculty, staff, and students.

Monitor network carefully: With the recent proliferation of cyber-attacks and threats, network monitoring has likely become a regular activity within IT departments, performing vulnerability scan may be one technique that IT and cybersecurity staff use to assess risk.

Recovering from Threats:

The recovery process for a cyber incident should be focused on people, policies and technology. When designing plans for recovery, if operating systems have been disabled, either as a result of a cyber-attack and/or a protective measure, concerned staff will need to work to restore technology capabilities. They will also need to notify the people impacted, including faculty, staff, and students, about contingency plans that will be in place until capabilities are restored. Lastly, cybersecurity and emergency management teams should take steps to review, revise, train, and continually remind key stakeholders on policies that may be implemented to prevent future attacks.

Understand the Situation:

During this step in the planning process, IT, cybersecurity, and emergency management teams should ensure they understand potential cyber threats that may impact their Cyber community. Once potential threats are identified, planning teams should assess the cyber risk to their networks and systems and from there, identify the cyber vulnerabilities.

Plan Preparation, Review and Approval:

When finalizing the Cybersecurity Annex, it is recommended that emergency management teams addresses how the annex connects to state, county and/or municipal plans. The annex may also identify a chain of command for before, during, and after an incident, as well as roles, responsibilities, and contact information for key stakeholders in prevention, protection, mitigation, response, and recovery.

Plan Implementation and Maintenance:

Once the plan is finalized, it is important for CSE to train stakeholders. In this case, stakeholders include faculty and staff (IT, emergency management, academic, research, administrative, etc.), students, and visitors.

Consider conducting emergency drills and exercises related to cybersecurity that involve these key stockholders, as well as other partners who will support the CSE in the event of a cyber-incident.

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, manipulate official data on the personal computer.

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

(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.

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

(q) Smartphones are also vulnerable to cyber-threats and must be configured for their secure use.

(s) Change your email password regularly.

(t) 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 Smartphones 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) Sanitise all data by carrying out a virus scan before it is downloaded.

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

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

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

(ac) Old smartphones are to be disposed of in a secure manner.

(ad) Do not make smartphone devices as storage for personal data.

(ae) Note down the IMEI (International Mobile Equipment Identity) number of the smartphone in a safe location.

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

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

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

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

Section 3. 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

1 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 Infosec 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.

Reference:

AICTE Cyber Security Strategy for Higher Education Institutes

URL:

https://www.aicteindia.org/sites/default/files/cyber/AICTE%20Cyber%20Security%20Strategy%20for%20Higher%20Education%20Institutes.pdf