STUDENT INFROMATION CYBER SECURITY POLICY

2024 – 2025

Main Office: 440 Franklin Street, Suite 500
Bloomfield, NJ 07003
Phone: 973-746-8717
Fax: 973-746-8714

Intern Clinic: Suite 550
Phone: 973-746-2848
Fax: 973-746-2088

1.0 INTRODUCTION

The Eastern School of Acupuncture and Traditional Medicine's (ESATM) Cyber Security Policy is a formal set of rules by which those staff members who are given access to college technology and information assets must abide. The Cyber Security Policy serves several purposes. The main purpose is to inform school users: employees, contractors, and other authorized users of their obligatory requirements for protecting the technology and information assets of the college. The Cyber Security Policy describes the technology and information assets that we must protect and identifies many of the threats to those assets.

2.0 WHAT ARE WE PROTECTING?

It is the obligation of all users of the college systems to protect the technology and information assets of the college. This information must be protected from unauthorized access, theft, and destruction. The technology and information assets of the school are made up of the following components:

- Computer Hardware: CPU, disc, Email, web, application servers, PC systems, application software, system software, etc.
- System Software: including operating systems, database management systems, and backup and restore software, communications protocols, and so forth.
- Application Software: used by the various departments within the college. This includes custom written software applications, and commercial off the shelf software packages.
- Communications Network hardware and software including: routers, routing tables, hubs, modems, multiplexers, switches, firewalls, private lines, and associated network management software and tools.

2.1 Classification of Information

User information found in computer system files and databases shall be classified as either confidential or non-confidential. The college shall classify the information controlled by them.

3.0 DEFINITIONS

Chief Information Officer. The President/Chief Executive Officer shall serve as the Chief Information Officer.

Security Administrator. An authorized employee shall be designated as the Security Administrator for the college.

4.0 THREATS TO SECURITY

4.1 Employees

One of the biggest security threats is employees. They may do damage to your systems either through incompetence or on purpose. You must layer your security to compensate for that as well. You mitigate this by doing the following.

Management:

✓ Only give out appropriate rights to systems. Limit access to only business hours.

✓ When employees are separated or disciplined, you remove or limit access to systems.

✓ Advanced – Keep detailed system logs on all computer activity.

Employees:

✓ Do not share accounts to access systems. Never share your login information with co-workers.

✓ Physically secure computer assets, so that only staff with appropriate need can access.

4.2 Amateur Hackers and Vandals.

These people are the most common type of attackers on the Internet. The probability of attack is extremely high and there is also likely to be many attacks. These are usually crimes of opportunity. These

amateur hackers are scanning the Internet and looking for well-known security holes that have not been plugged. Web servers and electronic mail are their favorite targets. Once they find a weakness, they will exploit it to plant viruses or use the resources of your system for their own means. If they do not find an obvious weakness, they are likely to move on to an easier target.

4.3 Criminal Hackers and Saboteurs.
The probability of this type of attack is low, but not entirely unlikely given the amount of sensitive information contained in databases. The skill of these attackers is medium to high as they are likely to be trained in the use of the latest hacker tools. The attacks are well planned and are based on any weaknesses discovered that will allow a foothold into the network.

5.0 USER RESPONSIBILITIES
This section establishes usage policy for the computer systems, networks, and information resources of the office. It pertains to all employees and contractors who use the computer systems, networks, and information resources as business partners, and individuals who are granted access to the network for the business purposes of the college.

5.1 Acceptable Use
User accounts on college computer systems are to be used only for business of the college and not to be used for personal activities. Unauthorized use of the system may be in violation of the law, constitutes theft and can be punishable by law. Therefore, unauthorized use of the college computing system and facilities may constitute grounds for either civil or criminal prosecution.

Users are personally responsible for protecting all confidential information used and/or stored on their accounts. This includes their login IDs and passwords. Furthermore, they are prohibited from making unauthorized copies of such confidential information and/or distributing it to unauthorized persons outside of the college.

Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to college systems for which they do not have authorization.

Users shall not attach unauthorized devices on their PCs or workstations unless they have received specific authorization from the employees' manager and/or the college IT designee.

Users shall not download unauthorized software from the Internet onto their PCs or workstations.

Users are required to report any weaknesses in the college computer security, any incidents of misuse or violation of this policy to their immediate supervisor.

5.2 Use of the Internet
The college will provide Internet access to employees and contractors who are connected to the internal network ***and*** who have a business need for this access. Employees and contractors must obtain permission from their supervisor and file a request with the Security Administrator.

The Internet is a business tool for the college. It is to be used for business-related purposes such as: communicating via electronic mail with suppliers and business partners, obtaining useful business information and relevant technical and business topics.

The Internet service may not be used for transmitting, retrieving, or storing any communications of a discriminatory or harassing nature or which are derogatory to any individual or group, obscene or

pornographic, or defamatory or threatening in nature for "chain letters" or any other purpose which is illegal or for personal gain.

5.3 Monitoring Use of Computer Systems
The college has the right and capability to monitor electronic information created and/or communicated by persons using college computer systems and networks, including email messages and usage of the Internet. It is not the college's policy or intent to continuously monitor all computer usage by employees or other users of the college's computer systems and network. However, users of the systems should be aware that the college may monitor usage, including, but not limited to, patterns of usage of the Internet (e.g., site accessed, on-line length, time of day access), and employees' electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and with college policy.

5.4 Awareness and Notification
All employees should make every effort to Identify, Avoid, and Report suspicious activity, email, warnings, alerts etc.

6.0 ACCESS CONTROL
A fundamental component of our Cyber Security Policy is controlling access to the critical information resources that require protection from unauthorized disclosure or modification. The fundamental meaning of access control is that permissions are assigned to individuals or systems that are authorized to access specific resources. Access controls exist at various layers of the system, including the network. Access control is implemented by logon ID and password. At the application and database level, other access control methods can be implemented to further restrict access. The application and database systems can limit the number of applications and databases available to users based on their job requirements.

6.1 User System and Network Access – Normal User Identification
All users will be required to have a unique login ID and password for access to systems. The user's password should be kept confidential and MUST NOT be shared with management and supervisory personnel and/or any other employee whatsoever. All users must comply with the following rules regarding the creation and maintenance of passwords:

- Password must not be found in any English or foreign dictionary. That is, do not use any common name, noun, verb, adverb, or adjective. These can be easily cracked using standard "hacker tools".
- Passwords should not be posted on or near computer terminals or otherwise be readily accessible around the terminal.

Users are not allowed to access password files on any network infrastructure component. Password files on servers will be monitored for access by unauthorized users. Copying, reading, deleting, or modifying a password file on any computer system is prohibited.

Users will not be allowed to logon as a System Administrator. Employee Login IDs and passwords will be deactivated as soon as possible if the employee is terminated, fired, suspended, placed on leave, or otherwise leaves the employment of the college.
Employees who forget their password must notify the IT department to get a new password assigned to their account.
Employees will be responsible for all transactions occurring during login sessions initiated by use of the employee's password and ID. Employees shall not login to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.

6.2 System Administrator Access

System Administrators, network administrators, and security administrators will have administrative access to host systems, routers, hubs, and firewalls as required to fulfill the duties of their job.
All system administrator passwords will be ***DELETED*** immediately after any employee who has access to such passwords is terminated, fired, or otherwise leaves the employment of the college.

6.3 Connecting Devices to the Network
Only authorized devices may be connected to the college network(s). Authorized devices include PCs and workstations owned by the college that comply with the configuration guidelines of the college. Other authorized devices include network infrastructure devices used for network management and monitoring. Users shall not attach to the network: non-college computers that are not authorized, owned and/or controlled by school.
NOTE: Users are not authorized to attach any device that would alter the topology characteristics of the Network or any unauthorized storage devices, e.g., thumb drives and writable CDs.

6.4 Remote Access
Only authorized persons may remotely access the college network. Remote access is provided to those employees, contractors and business partners of the college that have a legitimate business need to exchange information, copy files or programs, or access computer applications. Authorized connection can be remote PC to the network or a remote network to college network connection. The only acceptable method of remotely connecting into the internal network is using a secure ID.

6.5 Unauthorized Remote Access
Users may not install personal software designed to provide remote control of the PC or workstation. This type of remote access bypasses the authorized highly secure methods of remote access and poses a threat to the security of the entire network.

7.0 PENALTY FOR SECURITY VIOLATION
The college takes the issue of security seriously. Those people who use the technology and information resources of ESATM must be aware that they can be disciplined if they violate this policy. **Upon violation of this policy, an employee of ESATM may be subject to discipline up to and including dismissal.** The specific discipline imposed will be determined by a case-by-case basis, taking into consideration the nature and severity of the violation of the Cyber Security Policy, prior violations of the policy committed by the individual, state, and federal laws and all other relevant information. Discipline which may be taken against an employee shall be administrated in accordance with the appropriate rules or policies detailed in the Handbook.

8.0 SECURITY INCIDENT HANDLING PROCEDURES
This section provides some policy guidelines and procedures for handling security incidents. The term "security incident" is defined as any irregular or adverse event that threatens the security, integrity, or availability of the information resources on any part of the college's network. Some examples of security incidents are:

- Illegal access of a college's computer system. For example, a hacker logs into a production server and copies the password file.
- Damage to a college computer system or network caused by illegal access. Releasing a virus or worm would be an example.
- Denial of service attack against a college web server. For example, a hacker initiates a flood of packets against a Web server designed to cause the system to crash.
- Malicious use of system resources to launch an attack against other computer outside of the college's network. For example, the system administrator notices a connection to an unknown network and a strange process accumulating a lot of server time.

Employees, who believe their terminal or computer systems have been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to the President/CEO immediately. The employee shall not turn off the computer or delete suspicious files. Leaving the computer in the condition it was in when the security incident was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem.