**Workstation Security Policy**

**Purpose:**

It is the policy of Trialomics, Inc to safeguard the confidentiality, integrity, and availability of protected health information (PHI), business and proprietary information within its information systems by controlling access to these systems/applications. As such, this policy describes the different workstation security requirements of the organization.

**Policy:**

1. Access to information systems by all users is allowable only on a minimum necessary basis.
2. All users are responsible for reporting an incident of unauthorized access of the organization’s information systems.
3. The same levels of confidentiality that exist for hard copy PHI, business, and proprietary information apply to digital and/or electronic protected health information (ePHI) within the organization’s information systems and are extended even after termination or other conclusion of access.
4. Automatic Logoff
   1. Users are required to make information systems inaccessible by any other individual when unattended by the user, such as locking or logging off the systems; if the device is used only by a single individual with a unique log in, it may be locked.
   2. Users must log off information systems/applications at the end of their shift, or at the end of their need to use the system/application, whichever is sooner.
   3. The Security & Privacy Officers shall approve exceptions to automatic log off requirements.
5. Workstation Use
   1. Workstations should only be used for authorized business purposes.
   2. Workstations should be encrypted.
   3. When possible, workstations should be placed in secure areas.
   4. Workstations in patient rooms or public areas must be logged off or locked when not in use.
   5. Users must take actions to prevent unauthorized viewing, such as privacy screens, minimizing sessions, closing laptops, etc.
   6. All users are responsible for practicing precautions to protect the confidentiality, integrity, and availability of ePHI in the information systems at all times.
   7. Workstations may not be used to engage in any activity that is illegal or is in violation of organization’s policies.
      1. Access may not be used for transmitting, retrieving, or storage of any communications of a discriminatory or harassing nature or materials that are obscene or “X-rated”.
      2. No messages with derogatory or inflammatory remarks about an individual’s race, age, disability, religion, national origin, physical attributes, sexual preference, political affiliation, or health condition shall be transmitted or maintained.
      3. No abusive, hostile, profane, or offensive language is to be transmitted through the organization's system.
   8. Information systems/applications also may not be used for any other purpose that is illegal, unethical, or against company policies or contrary to organization’s best interests.
      1. Messages containing information related to a lawsuit or investigation may not be sent without prior approval.
   9. Solicitation of non-company business, or any use of organization’s information systems/applications for personal gain is prohibited.
   10. Participation in chain letters and other such activities is also prohibited.
   11. Transmitted messages may not contain material that criticizes Trialomics, Inc, its providers, its employees, or others.
   12. Users may not misrepresent, obscure, suppress, or replace another user’s identity in transmitted or stored messages.
6. Workstation Security
   1. Workstations might not be the property of Trialomics, Inc
   2. Workstations are protected with security controls
   3. Users may access and utilize workstations as deemed necessary..
   4. All users must report unauthorized workstation use to the Security Officer or designee.
   5. Users will install anti-virus software on all workstations to prevent transmission of malicious software. This anti-virus software is regularly updated.
   6. Networks are secured with a Firewall.
   7. Network access is limited to legitimate or established connections. An established connection is return traffic in response to an application request submitted from within the secure network.
   8. Firewall console and other management ports are appropriately secured or disabled and are located in a physically secure environment.
   9. Mechanisms to log failed access attempts are in place.
      1. Trialomics, Inc will receive notifications on each failed login attempt.
   10. The configuration of firewalls used to protect networks is approved by the Security Officer or designee and maintained by the IT Department.
   11. Firewalls will be maintained as staff change positions.
   12. Servers are located in a physically secure environment and are on a secure network with firewall protection.
   13. The system administrator or root account is password protected.
   14. A security patch and update procedure is established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.
   15. All unused or unnecessary services are disabled.