[Insert Company Name and Logo]	
Title: Endpoint Protection	**P&P #:**
Approval Date:	**Review:**
Effective Date:	**Security Team**

Purpose: This policy describes security requirements for the organization’s endpoint IT devices.

Scope: This policy applies to all employees and other workforce members (whether paid, volunteer or contractor) having access to a workstation connected to the information technology infrastructure owned by our organization.

Procedure:

1. Access to information systems by all users is allowable only on a minimum necessary to perform work tasks.
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 sensitive and regulated data, business, and proprietary information apply to digital and/or electronic data within the organization’s information systems and are extended even after termination or other conclusion of access.
4. Automatic Logoff
    a. 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.
    b. 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.
    c. Information systems should automatically log users off the systems after [5] minutes of inactivity. (Each organization must choose the number of minutes for automatic logoff based on its risk analysis.)
        i. Shortened automatic log off times should be implemented for workstations located in public or high traffic areas or for portable devices.
    d. The Security & Privacy Officers shall approve exceptions to automatic log off requirements.

5. Workstation Use
    a. Workstations should only be used for authorized business purposes.
    b. When possible, workstations should be placed in secure areas.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

   c. Workstations in patient rooms or public areas must be logged off or locked when not in use.
   d. Users must take actions to prevent unauthorized viewing, such as privacy screens, minimizing sessions, closing laptops, etc.
   e. All users are responsible for practicing precautions to protect the confidentiality, integrity, and availability of sensitive and regulated data in the information systems at all times.
   f. Workstations may not be used to engage in any activity that is illegal or is in violation of organization’s policies.
      i. 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”.
      ii. 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.
      iii. No abusive, hostile, profane, or offensive language is to be transmitted through organization’s systems or applications.
   g. 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.
      i. Messages containing information related to a lawsuit or investigation may not be sent without prior approval.
   h. Solicitation of non-company business, or any use of organization’s information systems/applications for personal gain is prohibited.
   i. Participation in chain letters and other such activities is also prohibited.
   j. Transmitted messages may not contain material that criticizes [Insert Company name], its providers, its employees, or others.
   k. Users may not misrepresent, obscure, suppress, or replace another user’s identity in transmitted or stored messages.

6. Workstation Security
   a. Workstations are the property of [Insert Company name] and must always remain on the premises, unless prior authorization by the Security Officer or other designee has been granted for removal of workstations from the premises.
   b. Workstations utilized off organization’s premises are protected with security controls equivalent to those for on-site workstations.
   c. Users may only access and utilize workstations as assigned by their supervisor.
   d. Supervisors are responsible for monitoring use of workstations.
   e. All users must report unauthorized workstation use to the Security Officer or designee.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

f. [Insert Company name] will install anti-virus software on all workstations to prevent transmission of malicious software. This anti-virus software is regularly updated.

g. Portable workstations are also subject to the same safeguards and protections.

h. Portable workstations are maintained in a safe and secure manner when transported.

i. Any portable device that contains sensitive and regulated data must be encrypted.

    i. Portable media is also subject to the same requirements.

j. Networks are secured with a Firewall.

k. 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.

l. Firewall console and other management ports are appropriately secured or disabled and are in a physically secure environment.

m. Mechanisms to log failed access attempts are in place.

    i. [Insert Company name] will lock accounts after [3] failed login attempts. (Each organization must choose the number of failed login attempts based on its risk analysis.)

n. The configuration of firewalls used to protect networks is approved by the Security Officer or designee and maintained by the IT Department.

o. Firewalls will be maintained as staff change positions.

p. Servers are located in a physically secure environment and are on a secure network with firewall protection.

q. The system administrator or root account is password protected.

r. A security patch and update procedure are established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.

s. All unused or unnecessary services are disabled.

Violations:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Violation may also result in civil and criminal penalties to [Insert Company name] as determined by federal and state laws and regulations related to loss of data.

Attachments: None

Related Policies: None

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.