Section Name: Information Security Effective Date: September 3, 2019
Section Number: 800
Policy Number: 809

Subject: Information Security Awareness and Training

Overview: This policy specifies an information security awareness and training program to inform and motivate all employees regarding their information risk, security, privacy and related obligations. Effective information security requires the awareness and proactive support of all employees.

Purpose: The purpose of this policy is to ensure that security awareness and training controls are in place to protect information systems and legally protected data (CJIS, IRS 1075, HIPAA, etc.) and ensure information availability, confidentiality, and integrity of data.

Scope: This policy applies throughout the organization, regardless of whether or not employees use the computer systems and networks, since employees are expected to protect all forms of information assets including computer data, written materials/paperwork and intangible forms of knowledge and experience. This policy also applies to third-party employees working for the organization whether they are explicitly bound (e.g. contractual terms and conditions) or implicitly (e.g. by generally held standards of ethics and acceptable behavior) to comply.

Statement of Policy:

A. An information security awareness program should ensure that all workers achieve and maintain a basic level of understanding of information security matters. These include those that are general obligations under various policies, standards, procedures, guidelines, laws, regulations, contractual terms plus generally held standards of ethics and acceptable behavior.

B. Additional training is appropriate for employees with specific obligations related to information security that are not satisfied by basic security awareness. For example Criminal Justice Information Services (CJIS), Health Insurance Portability and Accountability Act (HIPAA), IRS 1075 just to name a few. Such training requirements shall be identified in the employee training plans.

C. Security awareness and training activities should commence as soon as practicable after employees join Monroe County. The awareness activities/training should be maintained on a continuous basis thereafter in order to support a reasonably consistent level of awareness of current issues and challenges in this area.

Policy Compliance:

A. Responsibility-The County Administrator, Information Security Manager or designee is responsible for maintaining the policy and providing support and advice during its implementation. All Elected Officials/Judges/Department Heads, or their designee(s), are responsible for implementing the policies and procedures and ensuring staff and

contractors' compliance in their respective areas. The IT Department will verify compliance through various methods including but not limited to periodic walk-throughs, business tool reports, internal and external audits, etc.

B. Compliance measurement - The IT Department will verify compliance to this policy through various methods, including, but not limited to, business tool reports, internal and external audits.

C. Exceptions- Any exception to the policy must be approved by the IT Department, County Administrator, Elected Official, Judge or Department Head in advance.

D. Non-Compliance- A User found to have violated this policy may be denied, blocked, suspended, or have their access to the Monroe County network terminated by the Monroe County IT Department. Additional disciplinary action may be taken, up to and including termination of employment or contracts.

Definitions: None

Administrative Procedures: None

Legislative History of Authority for Creation or Revision:

Adopted pursuant to action of the Monroe County Board of Commissioners, dated September 3, 2019.