Information Security Policy Statement

Objective:

The objective of information security is to ensure the business continuity of Monroe County, Michigan general government operations and minimize the risk of damage to data stored and managed by the organization by instituting preventative measures against security threats and reducing the potential impact from any incidents.

Scope:

Every official and employee within the Monroe County organization is responsible for protecting the technology infrastructure and data contained within the infrastructure network. The Information Security Management Framework (ISMF) encompasses elected offices, statutory offices, millage funded offices and those functional work areas necessary for the business operations of county government.

This scope includes systems that are the direct responsibility of the Information Technology Department to provide support to the underlying operation, and the maintenance and management of internal, external and web based data.

The ISMF will be supported through policies and procedures that encompass the security requirements mandated at the state and federal level including but not limited to operational requirements in criminal justice, the Health Insurance Portability and Accountability Act, Governmental Accounting Standards Board, Office of Child Support, etc.

Policy:

The Policy Statement's goal is to protect the organization's informational assets against all internal, external, deliberate or accidental threats.

The Policy Statement ensures that the following will be protected against unauthorized access:

- Information

- Confidentiality of information
- Integrity of information

Additional goals of the Policy Statement include:

- Availability of information for business processes will be maintained
- Legislative and regulatory requirements will be met
- Business continuity plans will be developed, maintained and tested
- Information security training will be available to employees
- All actual or suspected information security breaches will be reported to the County Administrator, Information Security Manager or designee and will be thoroughly investigated

Policies and procedures will be enhanced, new ones developed as may be identified and maintained to support the Policy Statement, including virus control measures, passwords and continuity plans.

Business requirements for availability and retention of information and systems will be developed and maintained.

The County Administrator, Information Security Manager or designee is responsible for maintaining the Policy Statement 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 compliance in their respective areas.

Compliance with the Information Security Policy Statement and it's associated policies and procedures is mandatory – failure to do so may result in disciplinary action, up to and including discharge and /or possible legal action.

Legislative History of Authority for Creation or Revision:

Adopted pursuant to action of the Monroe County Board of Commissioners, dated March 6, 2018