Section Name: Information Security Effective Date: September 3, 2019
Section Number: 800
Policy Number: 807

Subject: Vulnerability Scanning

Overview: This policy aims to establish controls and processes for the identification and management of technical vulnerabilities and their associated risks to Monroe County information assets in order to avoid potential negative business impact.

Purpose: Vulnerability scanning management is a process by which the vulnerabilities identified through scanning are tracked, evaluated, prioritized and managed until the vulnerabilities are remediated or otherwise appropriately resolved. Managing the vulnerabilities identified during scans ensures that appropriate actions are taken to reduce the potential that these vulnerabilities are exploited and thereby reduce risk of compromise to the County's information.

Scope: The policy applies to all information and/or technical resources that are owned by, or in the custody of Monroe County.

Statement of Policy:

Periodic or continuous vulnerability assessment scanning of all supporting assets in Monroe County will be performed at least twice annually or more frequently if there are perceived threats. The IT Department will provide the results of the tests in detailed reports to the County Administrator. These reports shall be identified in a way that they are not provided in response to requests under the Freedom of Information Act ("FOIA"), and the County Administrator shall document the FOIA exception(s) that apply.

External and internal penetration testing will be performed at least twice annually, when there are changes to the infrastructure (i.e. firewall updates, new equipment, etc.), or when threats are perceived. The purpose of penetration tests are to verify that the security controls protecting Monroe County are working properly.

Any vulnerabilities discovered during a security assessment will be corrected by the IT Department. High risk vulnerabilities must be remediated within 14 days of being reported to the County Administrator. Medium risks must be remediated within 30 days and low risk within 45 days. If they cannot be resolved in that time, a remediation plan must be submitted and updated regularly until such time the vulnerability can be resolved.

Policy Compliance:

A. Responsibility-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.

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 exceptions to the policy must be approved by the IT Department and Department Head or Elected Official for whom the employee works.

D. Non-Compliance – An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or contract.

Definitions: NA

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.