Section Name: Information Security Effective Date: September 3, 2019
Section Number: 800
Policy Number: 808

Subject: Patch Management

Overview: Monroe County is responsible for ensuring the confidentiality and integrity of the data housed in its network. It has an obligation to provide appropriate protection against malware threats such as ransomware, viruses, Trojans and worms which could adversely affect the security of the system or its data. Regular application of vendor-issued critical security updates and patches are necessary to protect Monroe County's data. All electronic devices connected to the network, including servers, workstations, firewalls, network switches and routers, tablets, mobile devices and cellular devices require patching for functional and secure operations.

Purpose: Software is critical to the delivery of Monroe County services. This policy provides the basis for an ongoing and consistent system and application update policy that stresses regular security updates and patches to operating systems, firmware, and productivity applications. Regular updates are critical to maintaining a secure operational environment.

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

Statement of Policy:

A. General – all system components and software shall be protected from known vulnerabilities by installing applicable vendor supplied security patches. System components and devices attached to the Monroe County network must meet minimum security standards, as outlined in the "Minimum Security Standards for Network Devices Policy". Critical patches shall be installed as soon as practicable and not later than fifteen (15) days after release by the vendor. Other patches not designated as "critical" by the vendor shall be applied at the next scheduled maintenance of the equipment.

B. System and Application Patching – as security patches are released, the Monroe County IT Department will schedule their installation as quickly as possible utilizing unattended tools whenever possible. The regular application of critical security patches is reviewed as part of normal change management and audit procedures.

C. Exceptions – patches on production systems (e. g. servers and enterprise applications) may require complex testing and installation procedures. In certain cases, risk mitigation rather than patching may be preferable. The risk mitigation alternative selected should be determined through a risk outage vs. exposure comparison.

Administrative Procedures:

A. Security Patching Procedures: The process shall ensure that application, system, and network device vulnerabilities are:

    1. Evaluated regularly and responded to in a timely fashion
    2. Documented and well understood by support staff
    3. Automated and regularly monitored wherever possible
    4. Executed in a regularly scheduled manner and communicated accordingly
    5. Applied in a timely and orderly manner based on criticality and applicability of patches and enhancements

B. Audit Controls: Patch history will be maintained for all servers, routers, firewalls, switches, controllers and applications via logs maintained in the IT Department. In addition, tools will be used to compare current firmware and software versions against current industry standards.

C. Enforcement: Users found in policy violation may be subject to disciplinary action, up to and including termination.

Definitions:

A. Patch – a piece of software designed to fix problems with or update a computer program or its supporting data
B. Trojan – A class of computer threat (malware) that appears to perform a desirable function but in fact performs undisclosed malicious functions
C. Virus – A computer program that can copy itself and infect a computer without the permission or knowledge of the owner
D. Worm – A self-replicating computer program that uses a network to send copies of itself to other noes. May cause harm by consuming bandwidth
E. Ransomware - type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid.

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 area

B. Compliance measurement- The Monroe County IT Department will verify compliance to this policy through various methods, including but not limited to, business tool reports, and 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 - If compliance is not feasible or technically possible, or if a deviation is necessary to support a business function, then a request for exception will be filed with the IT Director and the head of the respective court, department or office noting the reason and an expected resolution date.

Legislative History of Authority for Creation or Revision:

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