Section Name: Information Security Effective Date: April 2, 2019
Section Number: 800
Policy Number: 804

Subject: Minimum Security Standards for Network Devices

Overview: Access to and use of network resources is a privilege and accorded at the discretion of Monroe County Government (the "County"). Devices connected to the County network (network), must comply with the minimum standards for security as set forth by the Monroe County IT Department. Elected offices and departments within the county may develop stricter standards for themselves. Devices that do not meet the minimum standards may be disconnected. Devices that host more sensitive or restricted data are required to conform to more rigorous standards as outlined by their respective state and federal agencies (CJIS, IRS, HIPAA, etc.)

Purpose: The purpose of this policy is to protect the County infrastructure, data stores, and all devices connected to the network. The standard is intended to prevent exploitation of County resources by unauthorized individuals, including the use of County resources by unauthorized individuals to attack other systems on the County or other attached networks or the internet.

Scope: This policy applies to any device that connects to the County network. It also applies to all employees, contractors, consultants, temporary staff, and other people or organizations who perform work for or at the County ("Users")

Statement of Policy:

A. Software Patch Updates – County networked devices must only run software for which security patches are made available in a timely fashion. All currently available patches must be applied on a schedule, appropriate to the severity of the risk they mitigate, unless otherwise determined by the IT Department.
B. Anti-malware and Anti-virus software – For all devices for which anti-malware and/or anti-virus is available, the version must be up-to-date. In addition, the software must run real-time scanning and/or scan the device regularly.
C. Host-based Firewall Software – For endpoint devices for which host-based firewall software is available, host-based firewall software must be running and configured to block all inbound traffic that is not explicitly required for the intended use of the device when the device is not connected directly to the County network. Use of a network-based firewall will be used when devices are connected to the Monroe County network.
D. Use of Authentication – Network devices and local (console) device access must require authentication by means of passwords/ passphrases or other secure authentication mechanisms unless the explicit purpose of the service/device is to provide unauthenticated access (for example: public web servers or public kiosks) and it can do so without readily allowing it to be used by attackers. Notably, the following network services must require authentication: proxy services, email (SMTP) relays, wireless access points, remote desktop, SSH shell access, and printer/network appliance administrative interfaces.

Simple devices like printers and networked attached storage, that do not support local authentication, but are in secure locations, are exempt from this requirement. In the event that a printer or NAS device is connected to the County Network via Ethernet or another hard link, all wireless connectivity must be disabled.

All County wireless access points must require strong encryption to associate (such as WPA2-Enterprise or WPA3), or use a captive portal or other strong mechanism approved by the IT department to keep unauthorized users within range from using it to get full access to the County network. WEP or MAC address restrictions do not meet this requirement.

E. Password/passphrase Complexity – passwords and passphrases must meet the guidelines as outlined in the *System Authentication Policy*.
F. Privileged Accounts – Privileged and super-user accounts (Administrator, root, etc.) must not be used for non-administrative activities. Network services must run under accounts assigned the minimum necessary privileges. Devices that do not support separate facilities for privileged or unprivileged access (e.g. some network appliances and printers with embedded operating systems) are exempt from this requirement.

Policy Compliance:

A. 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 April 2, 2019