Maryland DEPARTMENT OF INFORMATION TECHNOLOGY	Information Technology Policy and Standards	Approved: *Michael G. Leahy* 7820D075CBE64C5... Michael G. Leahy, Secretary	09/22/2020 Date
# 20-08	***IT Security Boundary Protection Baseline***		

Area(s):

☐ Process ☐ Procurement ☒ Security ☐ Hardware ☐ Web
☐ Facility ☐ End-User ☐ Software ☐ Network ☐ Data
☐ Voice ☐ Audit ☐ Other

Replaces Other Policy: ☒ No ☐ Yes

Purpose: Establishes the requirement that units within the Executive Branch must utilize a documented baseline standard for boundary devices, ensure that the standard is followed, and audit devices to ensure compliance.

Policy Statement: Having a documented baseline standard for boundary devices contributes to the organizational security by applying reasonable protections to both the device and for the rules that permit and deny traffic flows. Because these assets are exposed to external entities and users, it is imperative to ensure that appropriate protections are in place.

Therefore, units that operate boundary devices must create a documented baseline that describes the minimum configuration standards. This standard must include setting to protect the device itself, as well as rules to limit traffic, and standards for rule construction (e.g., Inbound rules must not specify "any" as a destination). Units must review and update the baseline semi-annually and internally perform and document an audit the configuration to ensure compliance with the standard annually.

DoIT will provide a copy of the approved baseline configurations for devices under DoIT management. Units that use the DoIT provided baseline are not required to maintain an independent baseline, however if they choose to do so, updates that negatively impact security must be approved. Configuration standards must be approved by the Office of Security Management.

Units have 90 days from the approval date of this policy to provide the Office of Security Management with a written copy of the baseline. Units that are unable to create and manage a documented baseline must develop a plan to migrate into DoIT managed firewall within 180 days of policy approval.

Applicable Law & Other Policy:
- MD State Finance and Procurement Code Ann. § 3A-301-309
- Governor's Executive Order 01.01.2019.07
- MD State Government Code §10-1301-1308
- MD State IT Security Manual, 2019
- NIST Cyber Security Framework: PR.IP-1, PR.PT-3
- NIST Special Publication 800-53: AC-3, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10

Scope and Responsibilities: All executive branch units of state government, except those identified in Maryland Code, SF&P § 3A-302. Agency executives, managers and staff shall ensure compliance with this policy.

Key Terms:

Department of Information Technology (DoIT): An executive branch unit of Maryland state government, organized according to Maryland Code, State Finance and Procurement Article, § 3A.

Policy: A statement of jurisdiction and methods to guide agencies in the management of IT resources and services.

<u>Units:</u> All executive branch units of state government, except those identified in Maryland Code, SF&P § 3A-302.

Technical Specifications: See the *Maryland State IT Security Manual*, Controls Section (pages 21-185), available at https://doit.maryland.gov/Documents/Maryland%20IT%20Security%20Manual%20v1.2.pdf

Policy Review: By the DoIT IT Policy Review Board annually or as needed.

Contact Information: Chair, IT Policy Review Board, doit-oea@maryland.gov 410-697-9724. The Policy #20-08 steward is the State Chief Information Security Officer.