Duke University Vulnerability Management Policy
University IT Security Office
Version 1.0

Authority:
Duke University Chief Information Officer
Duke Medicine Chief Information Officer
Duke University Chief Information Security Officer
Duke Medicine Chief Information Security Officer

1. Purpose
The purpose of this policy is to define the requirements for notification, testing, and installation of security-related patches on devices connected to Duke networks.

2. Policy
It is the stated goal of the Duke University and Duke Medicine to provide secure IT resources and services in order to protect institutional information assets, as well as the privacy of individual students, faculty, staff, patients, and other entities with which the institution has contractual obligations. In doing so, Duke University and Duke Medicine must comply with applicable laws, regulations, and other university or unit policies regarding protection of systems and data. The timely and consistent application of vendor-supplied security patches or mitigation of a reported vulnerability are critical components in protecting Duke University and Duke Medicine network, systems, and data from damage or loss due to threats such as worms, viruses, data loss, or other types of external or internal attacks.

Duke University and Duke Medicine authorized the IT Security Office and Information Security Office to conduct routine scans of devices connected to Duke University and Duke Medicine networks to identify operating system and application vulnerabilities on those devices.

Duke University and Duke Medicine require all administrators of systems connected to Duke networks to routinely review the results of vulnerability scans and evaluate, test and mitigate operating system and application vulnerabilities appropriately, as detailed in the Vulnerability Management Process. Should an administrator identify a reported vulnerability as a potential false positive, the appropriate security office should be engaged to verify.

3. Scope
This policy applies to all departments and schools of Duke University and Duke Medicine.

This policy applies to all electronic devices connected to Duke University or Duke Medicine networks (public and private) including but not limited to computer workstations and servers, network switches and routers, specialized laboratory equipment, etc.
4. Responsibilities
System and application administrators are responsible for assessment and application of security patches that impact systems under their management and supervision.

5. Exceptions
Requests for exceptions to this policy (requests to not scan a device) may be granted for systems with other security measures (e.g., network filtering, firewall, etc.) in place to mitigate risk.

Any requests must be submitted in writing to the appropriate CISO for review and approval. Exception requests must include:

- Why the scanning exception is being requested.
- Risk to the enterprise of not scanning the device.
- Mitigation controls that have been implemented, and date of implementation.
- End date for the exception (not to exceed 6 months from the request date).
- In the case of systems or applications managed by departmental or school IT staff, endorsement of the request by the relevant IT staff.

6. Enforcement
It is the responsibility of system and application owners to ensure that the policy described in this document is followed. IT administrators understand that the secure implementation of systems and applications is a critical part of Duke’s overall information security strategy.

The Duke University IT Security Office and the Duke Medicine Information Security Office are authorized to limit network access for devices that do not comply with this policy.

Review Frequency: Every 3 years
Updated: 3/12

References:
Duke University Data Classification Standard
Duke University Acceptable Use Policy
Duke University ITSO technical standards
HIPAA