University of New Haven

Policies and Procedures

Policy Title: Office of Information Technology Patch Management

Policy No.: 7900 Rev.: 0
Effective Date: September 1, 2018
Last Revision: September 1, 2018

Responsible Office: Office of Information Technology
Responsible Official: Associate Vice President for Technology & CIO

Contents

Scope

This policy applies to all the University of New Haven's servers, computers, tablets, mobile devices or any electronic device that may require operating or security related patching.

Policy Statement

The University of New Haven is responsible for ensuring the confidentiality, integrity, and availability its data and that of customer data stored on its systems. The University of New Haven has an obligation to provide appropriate protection against malware threats, such as viruses, Trojans, and worms which could adversely affect the security of the system or its data entrusted

on the system. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems within this scope.

Reason for the Policy

The purpose of this policy is to ensure that all University-owned devices are proactively managed and patched with appropriate security updates. In addition, this policy is intended to instruct and inform the University community about the change in end point computing.

Definitions

OIT: Office of Information Technology

Patch: A piece of software designed to fix problems with or update a computer program or its supporting data

Endpoint: a computer based device i.e. computer, laptop, tablet, mobile device that may connect to the network

Trojan: A class of computer threats (malware) that appears to perform a desirable function but in fact performs undisclosed malicious functions

Virus: A computer program that can copy itself and infect a computer without the permission or knowledge of the owner.

Worm: A self-replicating computer program that uses a network to send copies of itself to other nodes. May cause harm by consuming bandwidth.

Policy Sections

7900.1 Servers

All University owned servers are to be maintained with the latest security patches to their operating system and key applications.

7900.2 Endpoints

All University owned computers, tablets, laptops and similar devices are to be maintained

with the latest security patches to their operating system and key applications. Patches are to be downloaded as available on a daily basis to the Kace Systems Management Appliance. The Kace Systems Management Appliance is to be scheduled to apply patches to all endpoints on a weekly basis. Schedules are to be varied based on the categorization of the endpoint i.e. Faculty/Staff, Classroom, Lab, etc.

7900.3 Procedures

Servers are to be monitored for available patches using IBM Big Fix Software. Weekly monitoring of the available patches is to be performed. Available patches are to be reviewed for any possible conflict and applied to appropriate server(s) at next available maintenance window.
When applicable patches should be first applied to a test server and verified to not cause application conflict before applying to production environment.

7900.4 Responsibilities

Responsibility to oversee the patching of all servers and endpoints belongs to the Director of Networking/Systems Operations and under the direction of and reported to the CIO.

Monitoring of available patches, application and testing is the responsibility of all Systems Administration staff and is to be under the direction of and reported to the Director of Networking/Systems Operations.