STAMFORD INTERNATIONAL UNIVERSITY

The Difference is Real

A member of LAUREATE INTERNATIONAL UNIVERSITIES

PATCH MANAGEMENT POLICY

IT-P-016

Date: 28th March, 2016

Stamford International University ("STIU")
Patch Management Policy

Rationale

Stamford International University ("STIU") is responsible for ensuring the confidentiality, integrity, and availability its data and that of customer data stored on its systems. STIU 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.

Purpose

This document describes the requirements for maintaining up-to-date operating system security patches on all STIU owned and managed workstations and servers.

Scope

This policy applies to workstations or servers owned or managed by STIU. This includes systems that organizational data owned or managed by STIU regardless of location. The following systems have been categorized according to management:

- Linux servers managed by Infrastructure Maintenance & Engineering Team
- Microsoft Windows servers managed by Infrastructure Maintenance & Engineering Team
- Workstations (desktops and laptops) managed by Site Support Engineering Team

Policy Information

Responsible Office: Department of Information Technology, Stamford International University

Issued On: 28th March, 2016

Revision History

Revision Number	Document Number	Description	Effective Date
00	IT-P-016	New Release	3rd September, 2015
01	IT-P-016	Revision 1	28th Mach, 2016

Revision: The University reserves the right to change this policy from time to time. Proposed changes will normally be developed by the policy managers with appropriate stakeholders. The review entities have sole authority to approve changes to this policy.

Contents

Recommendations and Approvals

Drafted by:

Name:	Chavanath Chatchaiyan
Position:	Technology Services Manager, IT Stamford International University
Date:	28th March, 2016

Approved by:

Name:	Sourjya Sankar Sen
Position:	Director, IT Stamford International University
Date:	28th March, 2016

Name:	Jiro Takahashi
Position:	CFO, Laureate International Universities (Thailand)
Date:	28th March, 2016

Policy

Workstations and servers owned by STIU must have up-to-date operating system security patches installed to protect the asset from known vulnerabilities. This includes all laptops, desktops, and servers owned and managed by STIU.

Workstations

Desktops and laptops must have automatic updates enabled for operating system patches. This is the default configuration for all workstations built by STIU. Any exception to the policy must be documented and forwarded to the Office of the CISO for review. *See Section on Exceptions*.

Servers

Servers must be regularly updates with latest service packs, hotfixes, and patches required to ensure the security of the STIU asset and the data that resides on the system, except for cases where deployment of such patches will obstruct normal operation of Applications hosted on the server. Any exception to the policy must be documented and forwarded to the Office of the CISO for review. *See Section on Exceptions*.

Roles and Responsibilities

- Infrastructure Maintenance & Engineering Team will manage the patching needs for the Linux, Unix, and Solaris servers on the network.
- Infrastructure Maintenance & Engineering Team will manage the patching needs for the Microsoft Windows servers on the network.
- Site Support Engineering Team will manage the patching needs of all workstations on the network and ensure all system images maintained are up to date with the latest patches.
- Information Security is responsible for routinely assessing compliance with the patching policy and will provide guidance to all groups in issues of security and patch management.
- The Change Management Board is responsible for approving the monthly and emergency patch management deployment requests.

Patch Management Methodology

Microsoft's System Center Configuration Manager (SCCM) is utilized to deploy patches. The entire patch management infrastructure is managed, updates can be controlled, reports can be run and vulnerability information can be displayed through SCCM.

Patch approval will take place at the primary SCCM server (upstream), while the actual deployment will take place through secondary update servers (downstream) at individual sites.

Patches will be deployed on Wednesday of every week. Missed schedules will be run on the next business day.

Appendix A outlines the topology of STIU's Patch Management Infrastructure.

Auditing and Monitoring

Active patching teams noted in the Roles and Responsibility section are required to compile and maintain reporting metrics that summarize the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk. These reports shall be made available to Information Security and Internal Audit upon request.

Enforcement

Implementation and enforcement of this policy is ultimately the responsibility of all employees at STIU. Any system found in violation of this policy shall require immediate corrective action. Violations shall be noted in the STIU's helpdesk system and support teams shall be dispatched to remediate the issue. Repeated failures to follow policy may lead to disciplinary action.

Exceptions

Exceptions to the patch management policy require formal documented approval from the Office of the CISO. Any servers or workstations that do not comply with policy must have an approved exception on file with the CISO.

Policy Review

The policy shall be reviewed after every year or as and when the need arises.

APPENDIX A: Topology of Patch Management Infrastructure