Procedure: Computer Patch Management Procedures

Procedure: 06/17/2010

1.0 Purpose

The purpose of this document is to describe the procedure for automated software updates to CCBC computers. Referred in the industry as patch management, a well planned and documented management update process will produce a fleet of stable and consistently configured desktop computers that are secure against known vulnerabilities to the computer operating system and application software. This document describes procedures used by the CCBC Information Technology Services (ITS) department to achieve these goals. This procedure document is intended for all CCBC faculty and staff.

2.0 Patch Management Strategy

Following Microsoft standards and industry best practices, the CCBC patch management strategy will be automated and will be applied to all College servers, laptop computers, and desktop workstations connected to the College network. The update process will be performed during off hour periods. The technical process will involve an automated wakeup of computers, an automated update of the computers, and an automated shutdown of the computers when the update process has completed. This strategy will minimize disruption to College operations and will ensure that updates are consistently performed.

3.0 Patch Management Process

Microsoft releases patches on the second Tuesday of every month. Microsoft may also release patches outside of this schedule, typically for high importance patches. On the Monday prior to the Tuesday release day each month, a pre-release notification list is made available by Microsoft. The following describes the patch severity rating as defined by Microsoft.

Microsoft Severity Rating System:
Critical - A vulnerability whose exploitation could allow the propagation of an Internet worm without user action.
Important - A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of user's data, or of the integrity or availability of processing resources.
Moderate - Exploitability is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation.

CCBC
The Community College of Baltimore County

Computer Patch Management Procedures

Low - A vulnerability whose exploitation is extremely difficult, or whose impact is minimal.

The CCBC patch management environment consists of a primary Windows Server Update Service (WSUS) server and three (3) patch staging servers, one for each College campus. The WSUS server is configured and registered to use the Microsoft automated patch notification service. The CCBC WSUS server checks the Microsoft patch service site daily for any available patches. Patches on the Microsoft site labeled critical are immediately downloaded.

Critical patches released by Microsoft address problems of immediate importance, typically related to Internet and email based threats. Critical patches will be tested and applied to the CCBC environment as soon as possible after release by Microsoft, utilizing the Emergency Change Management process. Critical patch updates submitted through Change Management will have associated contingency and back out plans. The Helpdesk will be notified through the Change Management process of all planned critical patch deployments.

All Low, Moderate, Important, and Critical patches released by Microsoft are downloaded to the WSUS server. The CCBC patch management review team will convene to review and approve which patches are to be released. The Patch Management team will be made up of the Director of Networks and Infrastructure, Manager of Systems Engineering, Manager of Network Engineering and Information Security, and the Helpdesk Manager. This team is responsible for evaluating patches to determine relevance in the CCBC environment.

On the second Wednesday of each month patches will be deployed to a patch test group. The test group will validate desktop software patches before College-wide deployment. The test group includes the following:

- Chief Information Officer
- Director of Networks and Infrastructure
- Systems Engineering Team
- Engineering and Information Security Team
- Help Desk Manager
- Help Desk Leads of all Campuses and Extension Centers
- Manager of Systems Development
- Manager of Database Administration
- 3 workstations in H-204

CCBC
The Community College
of Baltimore County

Computer Patch Management Procedures

Patch updates to College workstations and servers for low, moderate, important, and critical patches are performed accordingly to the following schedule.

Workstations

- 2nd week of each month – testing of patches
- 2nd Saturday of each month - Essex campus
- 3rd Saturday of each month - Catonsville, Hunt Valley and Owings Mills
- 4th Saturday of each month - Dundalk campus

Servers

- 2nd Friday of each month – SUS-ALPA group will be updated at 10pm.
- 3rd Tuesday of each month – Critical1 group will be updated at 3am.
- 3rd Wednesday of each month – Critical2 group will be updated at 3am.
- 3rd Thursday of each month – Critical3 group will be updated at 3am.
- 3rd Friday of each month – Critical4 group will be updated at 3am.
- 3rd Friday of each month – SUS-BETA group will be updated at 10pm.
- 4th Friday of each month – SUS-CHI group will be updated at 10pm.

The SharePoint, LDAP and Exchange servers will be done manually on the fourth Friday at 11pm. This is to ensure a controlled deployment with minimal problems.

Service Packs will not be automatically deployed but will be reviewed at semester break intervals to ensure the College stays within supported versions and service packs without disruptions to the academic environment.

WSUS reports, including exception reports, will be reviewed by the Systems Engineering team. Exceptions to the update process will be reported through the formal Change Management process.

Approved by Sr. Staff 06/29/10