21st Century Insurance
21st.com 1-800-211-SAVE

SMS 2003

SECURITY UPDATE MANAGEMENT PROCEDURES

Owner: IS / Microsoft Server Group

REVISION PAGE

Revision No.	Date	Comments	Owner
1.0	April 14, 2005	Initial Version	
1.1	April 28, 2005	▪ Updated to current status of Action Items ▪ Edited for accuracy and organization	
1.2	May 11, 2005	Edited per input from Microsoft technical consultant Greg Feiges	
1.3	May 24, 2005	Edited per input from Faizan Khan, Sean McMorrow	
1.4	June 7, 2005	Final version	

SMS 2003 Security Update Management Procedures

Table of Contents

1. Document Purpose and Scope 1

2. Project Purpose and Scope 1

3. Background 1

4. Policies 2

4.1. Baselining 2

4.2. Sarbanes-Oxley Compliance 2

5. Project Stakeholders 2

6. Roles and Responsibilities 3

7. New Procedure: Tasks and Scheduling 4

8. Setup Tasks 6

9. Interim and Ongoing Tasks 9

10. Maintenance 9

10.3. Non-Microsoft Security 9

10.4. Communications 10

11. Attachments 10

11.1. Patch Management Lead checklist 10

SMS 2003 Security Update Management Procedures

1. Document Purpose and Scope

This document describes procedures currently under development for managing Microsoft-issued security updates ("patches") to Windows server software. It covers organizational and technical aspects of improving and maintaining Microsoft Server Group's (MSG's) update management process. It is generally high-level and will ultimately be historical, as the procedures, once implemented, will be cyclical and documented or updated regularly elsewhere. After this document is signed off, changes should be made through amendments, not edits to the body of the document. Contact the Technical Writer to make an amendment.

2. Project Purpose and Scope

The objective of the SMS 2003 security update management procedures is to establish a repeatable, verifiable, thorough, and consistent method of applying security updates to Windows server software. The new procedures will extend or formalize the responsibilities of security update management to 21st Century Insurance departments and groups affected by it.

3. Background

Applying security updates to Windows server software poses numerous risks. Security updates can break applications, cause business interruptions by introducing regressions not discovered during the testing process, and introduce security vulnerabilities through patches that have themselves been hacked or issued by suspect sources. MSG has recognized the need to harden its current process and to enlist other departments within 21st Century as participants, notably Application Support groups and Security.

The process now in place and deemed less than optimal is documented as follows:

1. 21st receives update notification via e-mail from Microsoft.
   Microsoft sends these regularly, approximately once per month. Sonny Nguyen is the recipient.

2. Sonny evaluates all the updates described in the notification to see if they are relevant to the 21st environment.

3. After evaluation, Sonny discusses appropriate updates with IT's Security Group (Scott Thomas is manager).

4. After Security Group approval, IT opens Change Board request.
   The Change Board request lists 21st vulnerabilities and updates.

5. IT's Change Board Group (Jim Chalker head) evaluates the request and approves updates.

6. IT applies updates to the Dev environment.

7. After 24-48 hours on Dev, updates are applied to the Production environment.

Some of the overall tasks to be improved or introduced to 21st's process are:

1. Evaluating each update thoroughly before applying it

2. Submitting update application to Change Management process
3. Notifying application groups potentially affected by an update
4. Soliciting reports from Security
5. Establishing system health before applying updates
6. Performing acceptance testing on updates in App Support
7. Soliciting reports on results of acceptance testing
8. Piloting updates on Dev
9. Interdepartmental review of changes after updates are applied
10. Ongoing research of non-Microsoft information sources on update impact and possible hacks
11. Baselining updated images for new servers

Microsoft has provided a big picture of security update management summarized at 21st's SharePoint site, http://uncentshareptprd/sites/SMS2K3/Patch%20Management%20Process%20Improvement%20Documents/MSMSUB1.ppt.

4. Policies

For the time being, 21st will observe Microsoft's hierarchy of criticality for security updates. All "critical" and "important" updates will be applied to Production in the regular monthly security update procedure. All non-critical and non-important updates will be applied to the Dev environment on a monthly basis, and to Production on a quarterly basis. These non-criticals and non-importants will be applied to Prodution only after testing in the Dev environment. Details on scheduling, tasks, and responsibilities for the testing of non-important and non-critical updates is still TBD.

4.1. Baselining

The Patch Management Lead (see "Roles and Responsibilites" below) will establish a baseline for the image for new servers on a quarterly basis. The baseline will include all updates applied to Production. The PML will create a registry key for each quarterly baseline in order to maintain version control. Note that new servers will receive all the current patches.

4.2. Sarbanes-Oxley Compliance

All updates will be documented in compliance with Sarbanes-Oxley requirements. Reporting on the selection, testing, and rollout of each update will be available to all stakeholders on the SharePoint site.

5. Project Stakeholders

New responsibilities, new tasks, and new advantages will fall to:

- The Microsoft Server Group
- Application Support
- Security
- Change Board

6. Roles and Responsibilities

Role	Responsibility	Name	Secondary
Security	▪ Receive notifications on update processing to include notifications, availability, testing, and deployments ▪ Report on changes in threat level to Patch Management and/or SMS Lead	Robert Smith	N/A
MS Technology Account Manager (TAM)	Send update notification to 21st's MSG	Rob Choi	Rob Choi
SMS Admin/Lead	Install update, monitor update rollout	George Ibrahim	Sonny Nguyen
Patch Management Lead (PML)	▪ Identify update items to apply ▪ Manage all 21st notifications on update progress ▪ Determine which updates to apply and which to work around depending on results of App Support's acceptance testing (will become App Support's responsibility eventually)	George Ibrahim	Sonny Nguyen
Server Admin	Provide server and hardware support	MSG	George Ibrahim
App Support	▪ Provide application support ▪ Perform acceptance testing and report results ▪ Eventually: Determine which updates to apply and which to work around depending on results of acceptance testing	TBD for each app	TBD
Change Management Admin	Approve changes for Change Board	Jose Messina	Jesse Garcia
MS Technology Owners:			
Exchange	Provide administrative support for Exchange	Sonny Nguyen	MSG
SMS	Provide administrative support for SMS	George Ibrahim	Sonny Nguyen
Windows	Provide administrative support for Windows	MSG (Sonny Nguyen primary)	MSG
SharePoint	Provide administrative support for SharePoint	George Ibrahim	MSG
SQL	Provide administrative support for SQL	Stephen Wong, Eric Kim	MSG
IIS	Provide administrative support for IIS	Leo Sta Maria	MSG
MSG Change Authority	Review and approve change to submit to Change Board	Faizan Khan	Brooke Michaud
Technical Writer	▪ Summarize Change Board meetings ▪ Oversee changes to doc	Joan Maltese	Joan Maltese

7. New Procedure: Tasks and Scheduling

The following is a comprehensive checklist of the security update management tasks to be performed approximately monthly. The process starts at the beginning of the month.

Item #	Timeframe/ Deadline	Task
1.	Thurs 11:00 a	TAM e-mails MSG regarding likely update content (technologies involved, # of updates, all subject to change) for following Tuesday.
2.	Thurs 12:00 p	If no e-mail from TAM, PML calls TAM @ 714 396-7963.
3.	Thurs 1:00 p	PML checks ETC for relevance of security udpates to 21st.
4.	Thurs 2:00 p	PML submits Change Board Request to MSG Change Authority.
5.	Thurs 5:00 p	PML sends “heads-up” SharePoint notification to App Support, MSG technology owners, and Security. The notification includes a reminder to App Support to contact vendors for additional information on update impact, and instruction to raise any objections during or by Change Board Meeting Tuesday @ 4:00 pm.
6.	Thurs 5:00 p	PML posts TAM’s e-mail on SharePoint.
7.	Thurs 5:00 p	MSG Change Authority authorizes Change Board Request.
8.	Thurs through Mon 5:00 p	App Support posts availability issues regarding update to SharePoint, OR reports at Change Board Management meeting.
9.	Thurs through Mon 5:00 p	Security posts any change of threat level of update to SharePoint OR reports at Change Board Management meeting.
10.	Tues 11:00 a	TAM sends update bulletin to PML.
11.	Tues 11:30 am	If no e-mail from TAM, PML calls TAM @ 714 396-7963 OR checks microsoft.com.
12.	Tues 2:00 p	PML evaluates update notification for relevance to other technology owners.
13.	Tues 2:00 p	PML sends SharePoint notification to MSG technology owners, App Support, and Security of update and advises on reboot expectations.
14.	Tues 2:00 p	PML checks MS Client Health Monitoring tool log for health of client.
15.	Tues 2:00 p	PML fixes any client problems and enters incident in ETC.

Item #	Timeframe/ Deadline	Task
16.	Tues 2:00 p	Pilot to Dev. PML pushes update via SMS to the following no/low-risk Dev servers: HQS346 2K3 HQS607 2000 HQS302 NT4 and checks advertisement status.
17.	Tues 3:00 p	PML creates package for all Dev servers in DSUW (see Camtasia video for procedures, link TBD).
18.	Tues 4:00 p	PML presents change to Change Management Board.
19.	Tues 5:00 p	PML posts link to Microsoft bulletin on SharePoint.
20.	Tues 5:00 p	PML advertises package to Dev environment via SMS for non-business hours install (see Camtasia video for procedures, link TBD).
21.	Wed 8:00 a	PML sends “Dev update complete” SharePoint notification to App Support, Security, and MSG technology owners. Notification includes patches to be rolled out and note that PML must receive test results by 5:00 pm Thursday from App Support. No response will be considered no issues.
22.	Wed to Thurs 5:00 p	App Support performs acceptance testing, reports any results it considers significant to SMS Lead by 5:00 pm. (Goal is that App Support will recommend either deploying the binary or using a workaround based on test results; in the interim, the PML will make this decision.)
23.	Wed to Fri 5:00 p	PML modifies query in SMS2K3 for exclusions (ongoing based on Change Management decisions and acceptance testing). (See Camtasia video for procedures, link TBD.)
24.	Thurs 5:00 p	SMS Admin/Lead checks results of acceptance testing and modifies package as needed to remove all updates that did not pass testing in Dev and are not recommended for deployment by the application owners.
25.	Fri 9:00 a	SMS Admin/Lead advertises package to PROD collection scheduled for execution at 12:01am Sunday.
26.	Sun 12:01a	Production SMS collection executes advertisement and deploys update(s).
27.	Sun 2:00a	PML sends SharePoint “PROD updated” notification to App Support, Security, and MSG technology owners.
28.	Mon 10:00 a	SMS Admin/Lead monitors and reports on update rollout status.
29.	Mon 5:00 p	PML updates ETC if necessary.
30.	Tues, Wed, or Thurs	ALL except TAM attend Security Update Change Review Discussion Board. Expectations, inputs, and outputs for this meeting are TBD.
31.	Thurs 5:00 p	Technical Writer posts Security Update meeting summary on SharePoint.

The charts below give a condensed version of these tasks, and a checklist for the Patch Management Lead (also in the Attachments section of this document).

Gantt chart Checklist


"Gantt chart.xls"


Checklist.xls

8. Setup Tasks

Before the new procedures can be implemented, tools and infrastructure must be set up and other departments must enlist as participants. The tasks to accomplish this include:

Action Item	Owner	Due Date	Status
Preparation/Investigation			
1. Meet with Microsoft technicians to develop security update management process.	MSG	3/16 – 3/19	*Done*
Groundwork - Technical			
2. Review and discuss simple OU structure with Microsoft Server Group	Faizan Khan	4/19/05	*Resolution: Additional training required*
3. Create simple OU structure in AD Workaround: create custom SMS query based on AD host description	George Ibrahim, Sonny Nguyen	4/22/05	*Resolution: workaround*
4. Move servers to appropriate OU	George Ibrahim, Sonny Nguyen	4/22/05	*Resolution: workaround*
5. TS installation of new SMS2K3 console and client health monitoring tool	George Ibrahim, Sonny Nguyen	05/06/05	*Done*
6. Develop an up-to-date server inventory by speeding up polling schedule of hardware inventory from once/week to once/day. *NOTE: Runs daily at midnight.*	George Ibrahim	04/14/05	*Done*
7. Get/apply Service Pack One.	George Ibrahim		*Done*

Action Item	Owner	Due Date	Status
8. Deploy MS Client Health Monitoring tool to check client health before applying update.	George Ibrahim, Sonny Nguyen	04/15/05	*Done*
9. Pick servers for Dev pilot push, one server for each OS. HQS346 2K3 HQS607 2000 HQS302 NT4	George Ibrahim	04/29/05	*Done*
10. Create DSUW procedure video	George Ibrahim	6/10/05	
11. Change AD host description entries	George Ibrahim	05/20/05	*Done*
12. Implement query to create custom SMS collection	George Ibrahim	05/20/05	*Done*
13. Create collection video	George Ibrahim	6/10/05	
14. Get SQL licenses for SMS servers	Sean McMorow	6/10/05	
15. Investigate custom SMS web reporting	Sean McMorrow, George Ibrahim	05/26/05	*Resolution: Not needed at this time*
16. Production ready SQL install on SMS servers	Stephen Wong	05/24/05	*Done*
17. SQL install clean-up	Stephen Wong	5/24/05	*Done*
18. AD host description changes (export and import from Hyena)	George Ibrahim	5/24/05	*Done*
19. Advanced client rollout ▪ List special remote control hosts/users (5/23/05) ▪ Build collections (Prod, Dev, and special) (5/25/05) ▪ Roll out Dev advanced client (5/26 – 5/29/05) ▪ Roll out Prod advanced client (5/31 – 6/1/05) ▪ Roll out special advanced client (5/31 – 6/1/05)	George Ibrahim	See left	*Done*

Security

20. I.D. sources outside Microsoft to check up on possible exploitation of vulnerabilities that updates are intended to fix.	Robert Smith	Week of 4/18	*Done*

See Section 8.1 on Non-Microsoft Security.

Procedural/Administrative

21. Modify ETC database: 1) determine which apps run on which servers, and 2) make app-server a mandatory field.	Stephen Wong, Sean McMorrow	Week of 4/18	*Done*
22. Complete role IDs.		Week of 4/25	*Done*
23. Modify Microsoft area of SharePoint site. *See Section 8.2 on Communication.*	George Ibrahim, Sean McMorrow	6/30/05	
24. Build form or otherwise develop means to confirm App Support's acceptance testing.	Sean McMorrow	6/30/05	
25. Develop template for SharePoint notifications.	Sean McMorrow	6/30/05	
26. Finish documentation	Joan Maltese	5/24/05	*Done*

Awareness

27. Training/awareness campaign for new SharePoint subscribers (App Support and Security).	Sean McMorrow	6/30/05	
28. Subscribe App Support, MSG technology owners, and Security to Microsoft area of SharePoint.	Sean McMorrow	App Support 6/30/05	*MSG and Security done*

This list is not complete and will be added to.

9. Interim and Ongoing Tasks

Information Services and MSG will cooperate on the following items beyond setup.

Action Item	Owner
1. Investigate quarterly application of all updates, including non-criticals. (Download all updates to safe area, keep separate directories for approved-critical and unapplied-non critical.)	Faizan Khan
2. Establish internal risk hierarchy that corresponds to Microsoft's to determine which changes should be applied.	Faizan Khan
3. Apply non-important and non-critical updates to Dev on a monthly basis.	PML
4. Perform acceptance testing of non-critical and non-important updates in Dev environment.	Application Support
5. Apply all non-important and non-critical updates that pass acceptance testing to Production and to image for new servers on a quarterly basis.	PML
6. Update images for new servers with all updates (including non-critical and non-important updates that pass TBD testing) on quarterly basis. Create registry key for each quarterly baseline.	PML

10. Maintenance

Security update management must be supported by continual updates to the knowledge base. Content and methods are discussed in this section.

10.3. Non-Microsoft Security

The following is a list of sites regularly checked by 21st Security. These sites usually cover all forms of security alerts and vulnerabilities for Unix, AIX, Linux, Microsoft, Oracle, PeopleSoft, etc. This list should be reviewed and updated on a quarterly basis.

<http://www.infosyssec.com/infosyssec/index.shtml>

<http://www.microsoft.com/security/default.mspx>

<http://www.us-cert.gov/cas/alerts/>

<http://www.windowsitpro.com/WindowsSecurity/Index.cfm?Ad=1>

<http://securityresponse.symantec.com/>

<http://xforce.iss.net/xforce/alerts>

<http://nsi.org/Computer/comalerts.html>

10.4. Communications

Communication and documentation for security update management will be centralized on SharePoint, at http://uncentshareptprd/sites/SMS2K3/default.aspx. This site will be used for:

- Subscribing and listing all participants
- Holding all documentation
- Listing all resources
- Managing all notifications
- Maintaining project history

11. Attachments

11.1. Patch Management Lead checklist

SMS 2003 Security Management Checklist
for SMS Admin/Lead and Patch Management Lead

Item	Task	Deadline	Result/Status
1	E-mail from TAM regarding patch content for following Tues received. If not, contact TAM @ 714 396-7963	Thurs 12:00 a	
2	Check ETC	Thurs 1:00 p	
3	Submit Change Board Request to MSG Change Authority	Thurs 2:00 p	
4	Post link to bulletin on SharePoint	Thurs 5:00 p	
5	Change Board Request approved	Thurs 5:00 p	
6	Send "Heads-up" SharePoint notification to App Support, MSG technology owners, and Security. Include 1) reminder to App Support to contact vendors for additional info on patch impact, and 2) instruction to raise any objections during or by Change Board Meeting Tues @ 4:00 p	Thurs 5:00 p	
7	Availability/application issues received from App Support	Mon 5:00 p	
8	Threat issues received from Security	Mon 5:00 p	
9	Patch bulletin from TAM received. If not, contact TAM @ 714 396-7963 OR check microsoft.com	Tues 11:30 a	
10	Evaluate patch notification for relevance to other technology owners	Tues 2:00 p	
11	Send SharePoint notification to MSG technology owners, App Support, and Security of patch	Tues 2:00 p	
12	Check MS Client Health Monitoring tool log, make fixes and enter incident in ETC as appropriate	Tues 2:00 p	
13	Pilot patch to HQS346 (2K3), HQS607 (2000), and HQS302 (NT4). Check advertisement status	Tues 2:00 p	
14	Create all-Dev package in DSUW	Tues 3:00 p	
15	Present change to Change Management Board	Tues 4:00 p	
16	Post link to bulletin on SharePoint	Tues 5:00 p	
17	Advertise package to DEV environment for 9:00 p install	Tues 5:00 p	
18	Send "DEV patch complete" SharePoint notification to App Support, Security, and MSG technology owners. Include instruction to App Support that no response will be considered no issues.	Wed 8:00 a	
19	Modify query in SMS2K3 for exclusions	Fri 5:00 p	
20	SMS Admin/Lead has checked results of acceptance testing and modified package as needed	Fri 5:00 p	
21	SMS Admin/Lead has advertised package to PROD collection	Sun 5:00 p	
22	Send SharePoint "PROD patched" notification to App Support, Security, and MSG technology owners	Sun 5:00 p	
23	Update ETC	Mon 5:00 p	