Patch Management Plan Examples

DISCLAIMER: Sample documentation provided in this section is for example only. Each department should develop their own documentation based on processes, requirements and risks which are unique to them.

Figure 1: Example of a Patch Management Plan demonstrates a document which outlines the essential elements required for a patch management plan. This document is intended to be a high level presentation of the patch management plan, and is not intended to provide plan details. However, it should include:

- Scope of the plan
- Description of inventory
- Tier testing structure
- Time lines for automated patching
- Priority ratings for systems
- Description of deployment procedure.

Other information that might be included in the patch management plan may include contact information for mangers and IT support staff (if required).

Figure 2: Example of a Computer Systems Inventory provides additional information about the computer systems included in the patch management plan. Information includes:

- Computer name
- Department
- System type
- Operating system
- Computer assignee
- Physical location
- Current usage

The inventory should reflect the appropriate amount of information for the purposes of the division. However, additional information may include:

- Computer asset tag
- Operating system version
- Software installed (with version information)
- IP address
- MAC address
- Domain or Workgroup information
- System information (such as system speed, disk size, and available space)
- Manufacturer information

As part of the multi-tier deployment, IT support staff need to have a mechanism to notify IT management and other affected staff of the impending deployment of a patch.

Figure 3: Example of text used for a patch advisory demonstrates that the details required for a patch deployment notification should include:

- Date of deployment
- Patch name(s)
- Source of patch
- Priority of patch
- System(s) affected
- Impact of vulnerability
- Time line for deployment

After patch testing has been completed and the patches are ready for deployment, all affected systems should be patched within seven days. Extending this interval has the potential of exposing the University computing resources to additional risk.

IT support staff are responsible for compiling patch management plan reports for IT management. These should include:

- A listing of patches deployed with installation reporting
- A listing by computer of uninstalled patches
- Documentation of issues or concerns
- Patch exceptions

IT management will use reports to assess the effectiveness of their patch management plan. Patch management progress should be reviewed, and obstacles resolved and updates charted on a continuous basis. ***Figures 4*** through ***Figure 7*** show how different vulnerabilities may be tracked and reported.

Figure 1: Example of a patch management plan

DIVISIONAL PATCH MANAGEMENT PLAN
(as of 2007)

Mission: To provide routine, automated patching to divisional workstations only (not servers) on the SDSU network.

Divisional System Information Necessary:
An inventory of all divisional workstations that includes for each system an identifier, such as property ID tag, the operating system, the IP or DHCP, owner of the asset and physical location.

An ongoing and updated reference as to whether an inventoried system is off the network and/or non-bootable to the network.

Inventoried systems are identified as members of groups or Tiers for patch deployment purposes. Deployment occurs in stages to divisional workstations. For example, members of Tier I are IT support and test systems, Tier II is a collection of systems used by IT representatives in each department (DAREs) and Tier III is the remainder of the division's workstations.

Timeline for Automated Patching:
Check daily, weekly and/or monthly for notifications of critical vulnerabilities applicable to the system environment;
Use the patch management software to receive notifications of critical operating system and application patches;
Confirm the updates that apply to the system environment which should be deployed;
Notify appropriate managers of pending updates to be deployed and advise of planned deployment dates to each Tier (staged process);
Upon approval to deploy updates, send notification to IT representatives in the Division departments;
Notification includes all update references (patch #) and dates of deployment to each Tier.

For emergency deployment of a critical patch if necessary a deployment of the patch would be done to all Tiers at once.

System criteria for patching is:
Workstations with Windows 2000, XP operating systems;
Workstations must be bootable on the network

Automated Deployment consists of:
A centralized server running a patch management application;
A workstation client as a patch agent on each workstation;
A database of all detected network workstations to provide dynamic information as to system status;
Central reporting output of all divisional system's status on a weekly basis;
Weekly review of the number of systems with outstanding patches that remain vulnerable.

Figure 2: Example of a Computer Systems Inventory

System Items State ID June 2007	*Dept*	*EquipType*	*Op Sys Win,Mac,Unix*	**Last Name**	**Bld**	**Room**	*System Status (surplus, off network)*
Computer1746	ENG	PC	Windows 2000	Smith	Building1	320	Off network
Computer1767	ENG	PC	Windows 2000	Johnson	Building1	320	
Computer1769	SALES	PC	Windows 2000	Jenkins	Building1	200	On network/In use
Computer1836	HR	Server	Windows	Email Server	Building1	116	On network/In use
Computer1837	SALES	PC	Windows XP	Jonston	Building1	200	On network/In use
Computer1840	SALES	PC	Windows XP	Jones	Building1	200	Off network
Computer1846	SALES	PC	Windows XP	Padilla	Building1	200	On network/In use
Computer1850	HR	Server	Windows	Print Server	Building1	116	
Computer1934	SALES	Server	No Selection	File Server	Building1	210	Spare
Computer1946	SALES	PC	Windows XP	Brown	Building1	200	On network/In use
Computer1991	SALES	PC	Windows 2000	Haddin	Building1	200	On network/In use
Computer1992	BIS	PC	Windows 2000	Petros	Building1	331	Off network
Computer1993	IT	PC	Windows 2000	Test1	Building1	Lab1	On network/In use
Computer1994	IT	PC	Windows 2000	Test2	Building1	Lab1	
Computer1995	IT	PC	Windows 2000	Test3	Building1	Lab1	
Computer1997	IT	PC	Windows 2000	Test4	Building4	Lab1	
Computer1998	IT	PC	Windows 2000	Test5	Building3	Lab1	
Computer1999	IT	PC	Windows 2000	Test6	Building4	Lab1	
Computer2000	ENG	PC	Windows 2000	Kimmet	Building1	320	On network/In use
Computer2001	IT	PC	Windows 2000	Sanders	Building3	420	Spare
Computer2002	IT	PC	Windows XP	Portello	Building3	409	On network/In use
Computer2003	IT	PC	Windows 2000	Little	Building4	105	On network/In use
Computer2004	IT	PC	Windows 2000	Evans	Building4	105	
Computer2005	HR	PC	Windows	Brighton	Building1	116	On network/In use
Computer2008	HQ	PC	Windows 2000	Tarquin	Building2	104	
Computer2009	HQ	PC	Windows 2000	LAB1	Building2	104	
Computer2010	HQ	PC	Windows 2000	LAB2	Building2	104	
Computer2011	HQ	PC	Windows 2000	LAB3	Building2	230	
Computer2012	HQ	PC	Windows 2000	LAB4	Building2	104	
Computer2013	HQ	PC	Windows 2000	LAB5	Building2	104	
Computer2014	HQ	PC	Windows 2000	LAB6	Building2	104	
Computer2015	HQ	PC	Windows 2000	LAB7	Building2	104	
Computer2016	HQ	PC	Windows 2000	LAB8	Building2	104	
Computer2017	HQ	PC	Windows 2000	LAB9	Building1	233	
Computer2018	HQ	PC	Windows 2000	LAB10	Building1	233	
Computer2020	IT	PC	Windows 2000	Edrige	Building1	220	On network/In use
Computer2021	IT	PC	Windows 2000	Simson	Building1	220	
Computer2029	SALES	PC	Windows XP	Pascal	Building1	200	On network/In use
Computer2030	IT	PC	Windows 2000	Hadley	Building1	226	Off network

Figure 3: Example of text used for a patch advisory

Division Patch Advisory

Advisory Date: June 14, 2007

MS Patch or SP #: MS07-030, MS07-031, MS07-032, MS07-033, MS07-034, MS07-035

Date Issued by Microsoft – June 12, 2007

Priority Assigned = Moderate, Important, Critical: Critical

Desktop System Platform(s) affected:

Windows XP SP2,
Windows XP SP1,
Windows 2000 SP4,
Windows Vista

Impact of Vulnerability: - Remote Code Execution

Description of Patch/SP:

http://www.microsoft.com/protect/computer/updates/bulletins/200706.mspx

Division Deployment

Effective Date to Depts: June 14 - 19

Deploy Dates to Division System Tiers:

Tier 1 - June 14
Tier 2 - June 15 - 18 (Dares, TNSHelpDesk)
Tier 3 - June 19

Implementer : Division IT Support

Figure 4: Example of Tracking Microsoft Patches

	A	B	C	AF	AG	AH	AI	AJ	AK	AL	AM	AN	AO	AP	AQ	AR	AS	AT	AU	AV	AW	AX	AY	AZ	BA	BB	BC	BD	BE	BF
1	Patch #	Date issued	# Pc's	12/20	12/27	1/3	1/7	1/17	1/24	1/31	2/7	2/14	2/21	2/28	3/7	3/14	3/22	3/28	4/4	4/11	4/18	4/25	5/2	5/9	5/16	5/23	5/30	6/6	6/13	6/20
29	MS05-049	10/11/2005	581	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
53	MS06-017	4/11/2006	642	10	10	8	6	4	4	4	6	6	7	7	7	7	8	8	8	8	8	7	6	9	8	4	1	1	1	1
61	MS06-025	R 6/27/2006	631	10	10	9	4	2	3	5	7	5	4	3	2	2	0	2	2	2	1	1	0	5	1	2	3	2	2	5
71	MS06-038	7/11/2006	617	x	x	x	x	x	x	3	3	3	3	3	3	3	3	3	2	2	2	2	1	1	1	1	0	0	0	1
80	MS06-047	8/8/2006	635	4	4	3	1	1	1	1	1	2	1	0	0	0	0	0	0	0	0	0	0	1	2	2	2	2	2	2
87	MS06-054	9/12/2006	653	4	4	4	2	4	4	5	6	5	7	7	7	7	7	7	7	7	7	6	6	8	9	9	9	9	9	9
88	MS06-056	10/11/2006	666	3	3	5	2	3	4	4	4	4	5	3	3	2	2	3	3	3	3	3	3	3	4	5	4	3	2	2
90	MS06-058	10/11/2006	666	10	10	11	7	5	5	5	6	7	9	8	9	8	8	8	8	8	8	0	7	11	12	15	14	13	11	9
95	MS06-065	10/11/2006	666	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1
99	MS06-069	11/14/2006	664	3	2	2	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	0	0	1
111	MS07-003	1/092007	554					7	4	3	4	5	4	4	7	4	3	3	0	3	3	3	3	2	2	3	2	1	3	2
112	MS07-004	1/092007	554					83	52	48	44	45	21	10	3	3	2	1	2	0	0	0	0	2	1	1	1	2	1	1
113	MS07-005	2/13/2007	625										10	5	7	3	1	0	3	0	0	0	2	1	1	1	1	1	1	1
120	MS07-012	2/13/2007	625										86	39	20	12	9	8	3	2	3	2	1	2	2	2	2	2	2	2
121	MS07-013	2/13/2007	625										196	106	61	41	34	32	17	15	18	14	11	10	11	11	9	9	10	9
125	MS07-017	4/3/2007	631																	11	10	13	7	11	11	10	5	4	6	3
128	MS07-020	4/10/2007	619																		50	23	12	18	16	13	7	5	5	3
129	MS07-021	4/10/2007	619																		50	23	12	14	12	9	5	3	3	1
130	MS07-022	4/10/2007	619																		50	23	12	13	9	5	3	2	3	1
131	MS07-023	5/8/2007	665																						43	38	31	14	10	9
132	MS07-024	5/8/2007	665																						36	33	27	13	10	9
133	MS07-025	5/8/2007	665																						41	39	30	14	10	9
137	MS07-029	6/12/2007	679																											12
138	MS07-030	6/12/2007	679																											12
139	MS07-031	6/12/2007	679																											66
141	MS07-033	6/12/2007	679																											98
142	MS07-034	6/12/2007	679																											119
143	MS07-035	6/12/2007	679																											179
144				426	363	300	201	334	251	223	204	193	1410	880	442	289	237	225	155	149	333	216	168	165	293	265	197	114	101	563
145																														
146	No patches released this month																													
147	3/5/07 modified patch install schedule to morning and afternoon																													
148	Patches reissued with a functionality patch, not a security patch.																													
149	Week 1 = how many systems vulnerable (wk1, day 2=T1, day 3=T2, day 7=T3)																													
150	Week 2 = how many systems not reporting (laptops, dormant, surplus, not rebooted)																													
151	Week 3 = email reminder of systems vulnerable																													
152	Week 5 = includes laptops/domant systems rebooted twice																													
153																														
154	MS05-049	Computer2013 ----user jsmith -- 146.244.119.93 -- Win2k - LAB machine - Vulnerabilities in Windows Shell - possible false positive or Internet explorer issues - I have a phone call in to Dave McKee																												
155	MS06-017	These machines/laptops appear to have XP office installed on them. Specifically there usually is an Office XP or OfficeXP frontpage in add/remove programs that **needs to be uninstalled**, but not in all cases.																												

The report shown in Figure 4 is a very useful mechanism for tracking the deployment of patches. The numbers in the columns AF to BF show the number of systems which are reporting as unpatched between the dates 12/20/2006 and 6/20/2007. In theory, the number of system reporting unpatched should become zero over time, but in practice this is not so easy.

For instance, on line 30; zero systems are reporting as unpatched from 12/20/2006 to 5/2/2007 (nearly 5.5 months), until on 5/9/2007, 1 system reports as unpatched. This single system may have been a desktop system that was turned off until this time, or perhaps a laptop system that was not in use on the University network for these months. Either way, the responsible IT manager will need to assess the potential risk and decide whether to commit resources to tracking down/patching this single system, or focus on the deployment of other patches.

Assessing the potential risk of an unpatched system involves understanding what the patch does. For instance, on line 62, the highlighting and an "R" are used to indicate that this is a reissued patch, and is not a security patch. This type of information assists the IT manager in deciding on a course of action in setting the priority for ensuring the deployment of this patch.

Decisions about exceptions that the IT manager makes can be noted on this report (as they are in lines 155 and 156).

The most important trend that the IT manager should be able to see on this report is progress. For instance, on line 122; 196 systems report unpatched on 2/21/2007. By 2/28/2007, the number of systems reporting unpatched has dropped to 106 (a 54% reduction in one week), to 61 the next week (a 57% reduction), to 41 the next week and so on.

Figure 5: Example of Tracking 3rd Party Software Patches

Patching Software	Date issued	3/7/	3/14	3/21	3/27	4/4	4/11	4/18	4/25	5/2	5/9	5/16	5/23	5/30	6/6	6/13	6/20
Adobe Reader 8.0	12/1/2006	467	234	200	192	172	153	141	137	135	135	134	132	125	123	99	**97**
KB-931836-cumulative time zone update for Microsoft Windows operating systems	2/7/2007	7	7	5	5	3	2	3	1	1	0	0	0	0	0	1	**0**
KB931667-Addressing the daylight saving time changes in 2007 using the Outlook Time Zone Data Update Tool	1/30/2007	11	3	4	3	2	3	5	4	2	4	4	3	2	1	3	**2**
Google Internet Tool Bar	1/1/2007	26	26	35	36	29	16	4	6	5	7	11	10	2	1	2	**1**

The IT manager also needs to be able to track patch management progress for non-security or 3rd party software as well. The report in Figure 5 demonstrates a way to do this.

Again, the numbers in the columns from 3/7 to 6/20 are systems that are reporting back as unpatched.

Figure 6: Tracking Microsoft Vulnerabilities by Computer

**********	6/6/2007	**********	**********	6/13/2007	**********	**********	6/20/2007	**********
Computer Name	Compliance	Vulnerable	Computer Name	Compliance	Vulnerable	Computer Name	Compliance	Vulnerable
Computer1746	89.71%	7	Computer1066	80.60%	13	Computer1746	87.04%	7
Computer1767	91.43%	6	Computer1746	89.06%	7	Computer1767	89.71%	7
Computer1769	91.43%	6	Computer1767	90.91%	6	Computer1769	86.79%	7
Computer1836	91.67%	6	Computer1769	90.91%	6	Computer1836	89.83%	6
Computer1837	91.67%	6	Computer1836	91.18%	6	Computer1837	91.43%	6
Computer1840	91.67%	6	Computer1837	91.18%	6	Computer1840	91.43%	6
Computer1846	90.74%	5	Computer1840	90.91%	6	Computer1846	91.18%	6
Computer1850	90.57%	5	Computer1846	92.16%	4	Computer1850	91.18%	6
Computer1934	90.57%	5	Computer1850	92.00%	4	Computer1934	91.43%	6
Computer1946	94.52%	4	Computer1934	92.00%	4	Computer1946	92.75%	5
Computer1991	92.86%	4	Computer1946	92.31%	4	Computer1991	93.06%	5
Computer1992	92.59%	4	Computer1991	94.12%	4	Computer1992	92.96%	5
Computer1993	92.31%	4	Computer1992	95.52%	3	Computer1993	93.15%	5
Computer1994	92.59%	4	Computer1993	94.64%	3	Computer1994	93.55%	4
Computer1995	94.44%	4	Computer1994	94.12%	3	Computer1995	93.85%	4
Computer1997	95.77%	3	Computer1995	94.83%	3	Computer1997	94.37%	4
Computer1998	95.71%	3	Computer1997	96.92%	2	Computer1998	94.12%	4
Computer1999	94.92%	3	Computer1998	97.14%	2	Computer1999	92.00%	4
Computer2000	97.10%	2	Computer1999	98.48%	1	Computer2000	94.37%	4
Computer2001	96.43%	2	Computer2000	98.51%	1	Computer2001	94.03%	4
Computer2002	97.26%	2	Computer2001	98.04%	1	Computer2002	94.03%	4
Computer2003	97.06%	2	Computer2002	98.55%	1	Computer2003	93.10%	4
Computer2004	97.14%	2	Computer2003	98.48%	1	Computer2004	94.03%	4
Computer2005	97.30%	2	Computer2004	98.48%	1	Computer2005	94.44%	4
Computer2008	98.44%	1	Computer2005	98.57%	1	Computer2008	94.44%	4
Computer2009	98.25%	1	Computer2008	98.46%	1	Computer2009	94.44%	4
Computer2010	98.59%	1	Computer2009	98.46%	1	Computer2010	94.29%	4
Computer2011	98.11%	1	Computer2010	98.46%	1	Computer2011	94.20%	4
Computer2012	98.57%	1	Computer2011	98.04%	1	Computer2012	94.20%	4
Computer2013	98.65%	1	Computer2012	98.36%	1	Computer2013	94.20%	4
Computer2014	98.51%	1	Computer2013	98.18%	1	Computer2014	94.20%	4
Computer2015	98.15%	1	Computer2014	98.51%	1	Computer2015	94.37%	4
Computer2016	98.46%	1	Computer2015	98.18%	1	Computer2016	94.03%	4
Computer2017	98.28%	1	Computer2016	98.48%	1	Computer2017	94.29%	4
Computer2018	98.08%	1	Computer2017	98.55%	1	Computer2018	94.37%	4
Computer2020	98.61%	1	Computer2018	98.44%	1	Computer2020	92.59%	4
Computer2021	98.59%	1	Computer2020	98.41%	1	Computer2021	93.10%	4
Computer2029	98.28%	1	Computer2021	98.46%	1	Computer2029	92.98%	4
Computer2030	98.55%	1	Computer2029	98.28%	1	Computer2030	94.52%	4
			Computer2030					

To get a high level view of patch management plan progress by individual computer, the IT manager might use a report similar to the one shown in Figure 6. Here, the IT manager can not only see the relative state of compliance of each computer (given by %), but also the number of vulnerabilities that remain on each system.

In this report, a system with the name "Computer1066" suddenly appears on 13th June 2007. Looking at previous weeks, the IT manager can see that this system does not appear before this date. Further investigation shows it to be a new system that was not full patched. By the following week, the system no longer appears on the list of systems with vulnerabilities.

Figure 7: Tracking Specific Vulnerabilities by Computer

Google Tool Bar --- 6/6/2007			Google Tool Bar --- 6/13/2007			Google Tool Bar --- 6/20/2007		
Computer	Dept	User Name & Function	Computer	Dept	User Name & Function	Computer	Dept	User Name & Function
Computer1992	ENG	Petros/Development	Computer1992	ENG	Petros/Development	Computer2009	HQ	LAB1/Testing
Computer1746	ENG	Smith/Development	Computer1746	ENG	Smith/Development	Computer2010	HQ	LAB2/Testing
Computer1767	ENG	Johnson/Development	Computer1767	ENG	Johnson/Development	Computer2011	HQ	LAB3/Testing
Computer2000	ENG	Kimme/Manager						
			Computer2008	HQ	Tarquin/Personal	Computer1993	IT	Test1/Testing
Computer2008	HQ	Tarquin/Personal	Computer2009	HQ	LAB1/Testing			
Computer2009	HQ	LAB1/Testing	Computer2010	HQ	LAB2/Testing	Computer2003	SALES	Little/Personal
Computer2010	HQ	LAB2/Testing	Computer2011	HQ	LAB3/Testing	Computer2004	SALES	Evans/Personal
Computer2011	HQ	LAB3/Testing	Computer2012	HQ	LAB4/Testing			
Computer2012	HQ	LAB4/Testing	Computer2013	HQ	LAB5/Testing			
Computer2013	HQ	LAB5/Testing						
			Computer1993	IT	Test1/Testing			
Computer1836	HR	Email Server						
Computer1850	HR	Print Server	Computer1991	SALES	Haddin/Personal			
Computer2005	HR	Brighton	Computer2029	SALES	Pascal/Personal			
Computer1993	IT	Test1/Testing						
Computer1994	IT	Test2/Testing						
Computer2001	IT	Sanders/Personal						
Computer2002	IT	Portello/Personal						
Computer2020	IT	Edrige/Personal						
Computer2021	IT	Simson/Personal						
Computer2030	IT	Hadley/Personal						
Computer1934	SALES	File Server/Customer Info						
Computer1946	SALES	Brown/Manager						
Computer1991	SALES	Haddin/Personal						
Computer2029	SALES	Pascal/Personal						

Finally, sometimes the IT manager may want to be able to track the patch management plan progress by a specific vulnerability.

In Figure 7, the report being used gives information about location, assigned user and usage. Such information is valuable to the IT manager when setting priorities for ensuring the Google Tool Bar is removed.

In this case, by 6/13/2007, it was decided that priorities should be the human resources department, all managers, and the information technology department (with the exception of one test machine to further research the vulnerability).

The next set of priorities included all user systems that were not used for testing. This was achieved by 6/20/2007, however, by then two more users had downloaded and installed the vulnerability.