IT 17.03: Patch Management Standards

Policy Authority

BTS Administrative Rule 2.01- Security Administrative Rule
BTS Administrative Rule 2.07- Virus Prevention and Recovery

Purpose

The City of Portland's patch management policy seeks to contain and minimize threats to its software and the information assets within said software by prioritizing assets and protecting the most critical assets first. This protection is accomplished in part by testing and applying relevant software patches. A patch management policy is also necessary to regularly distribute patches that address such issue related to the stability of hardware and software platforms. The City's patch management policy seeks to accomplish this goal by establishing:

- Scope
- Roles and Responsibilities
- Deployment Schedules

All critical security patches should be tested and applied to relevant systems within 30 days of their release.

Procedure

Scope

The patch management policy applies to BTS maintained servers, workstations, and network devices. Both operating system and applications that reside on BTS maintained servers, workstations, and network devices are in scope of this policy as well. These operating systems and applications include, but are not limited to:

- Network Devices- Routers (Cisco), Switches (Cisco), Load Balancers (F5), Firewalls (Juniper), Intrusion Prevention Systems (Tipping Point), Authentication Systems (RSA)
- Workstations- Laptops & Desktops (Windows XP, Microsoft Office, Adobe Acrobat)
- Servers- Windows Server 2000, 2003, SQL Server 2000, SQL Server 2005, ColdFusion, FusionReactor, Microsoft Internet Information Server (IIS), Apache Tomcat

Alterations to this list are made by the Information Security Manager.

Roles and Responsibilities

Assigned roles and responsibilities ensures accountability, provides strategic direction and coordinates conflict resolution

BTS's Information Security, Networking, Systems Support, Server Support, and Corporate Applications have important responsibilities to ensure that this patch management policy is successfully implemented. The table below illustrates the BTS roles and responsibilities associated with patch management:

Team/Division	Responsibilities
Information Security	-Determines patching policy -Sets patching performance metrics and timelines

	-Audits compliance
Systems Support	-Acquires and deploys patches for workstations (laptops and desktops). -Tests patches -Coordinates patch timelines with affected parties. -Reports and coordinates feedback on patch deployment
Server Support	-Acquires and deploys patches for servers. -Tests patches -Coordinates patch timelines with affected parties. -Reports and coordinates feedback on patch deployment
Corporate Applications	-Acquires and deploys patches for servers. -Tests patches -Coordinates patch timelines with affected parties. -Reports and coordinates feedback on patch deployment
Networking	-Acquires and deploys patches for network devices -Tests patches -Coordinates patch timelines with affected parties. -Reports and coordinates feedback on patch deployment

Within these teams or divisions, there are roles that hold certain responsibilities related to patch management. These roles and responsibilities are as follows:

Team/Division	**Role**	**Responsibilities**
Information Security	Information Security Analyst	-Facilitates patch management committee meetings. -Responsible for assessing and summarizing patching performance.
	Information Security Manager	-Sets patch management policy -Responsible for the creation of patch metrics -Approves exceptions to patch management process.
Systems Support	Testing Analyst	-Tests patches for stability and general impact on workstations -Reports testing results to patch deployment team
	Patching Administrator	-Acquires and deploys patches -Coordinates patch timelines with affected parties. -Reports to patch management committee on

		patch deployment efforts
Server Support	System Administrator	-Acquires and deploys patches -Coordinates patch timelines with affected parties. -Brings system back online after patch deployment and reboot. -Reports to patch management committee on patch deployment efforts
Corporate Applications	Application Administrator	-Acquires and deploys patches -Coordinates patch timelines with affected parties. -Brings system back online after patch deployment and reboot -Reports to patch management committee on patch deployment efforts

Patch Management Committee

A patch management committee should meet regularly to discuss the progress of patch management and be responsible for maintaining the accuracy of patching policies and procedures. The patch management committee should consist of at least one person from the following BTS teams and roles:

Team/Division	**Role**
Information Security	Information Security Analyst
Systems Support	Testing Analyst
	Patching Coordinator
Server Support	System Administrator
Corporate Applications	Application Administrator
Networking	Information Systems Analyst

Deployment Timelines

There are two categories of patch deployment:

- Emergency Release
- Scheduled Release

Emergency Release Patches

Emergency release patches are those patches that are deployed as soon as possible to combat a vulnerability that has been:

- Recognized in the broader Internet based computing environment, also known as “the wild” and/or
- Allows remote code execution on workstations or servers.

The Information Security team shall be responsible for identifying such situations and notifiying, via email the patch management committee, of the need to immediately release a given patch. The Information Security office identifies these type of patches primarily through:

- Microsoft's Security Response Center
- SANS Newsbites
- Vendor notification lists (email/rss)

Scheduled Release Patches

Scheduled release patches follow a pre-determined release sequence listed below.

In general, BTS will identify, evaluate, and deploy all "critical" vendor supplied security patches that are in scope within three weeks of their release. "Critical" vendor supplied security patches are divided into two categories:

- Microsoft Patches
- Non-Microsoft Patches

Microsoft Patches

In the case of Microsoft products, BTS deploys the security patches on the timetable listed below:

There are two categories of patch deployment:

- Emergency Release
- Scheduled Release

Microsoft Security Response Center (MSRC) Rating	Time to Deploy
Critical	4 weeks
Important	4 weeks
Moderate	10 weeks
Low	14 weeks

Non-Microsoft Patches

In the case of non-Microsoft patches, BTS deploys the security patches on the timetable listed below:

Common Vulnerability Scoring System (CVSS) Base Rating[1]	Time to Deploy
9-10	0 Day (Immediate)
7 to 8	1 Month
5-6.9	2 Months
3-5	3 Months
Less than 3	4 Months

Deployment Procedure

Patch Identification Process

BTS personnel within the Systems Support, Server Support, and Corporate Applications are primarily responsible for identifying the relevant patches for evaluation and deployment. Microsoft patches are identified through the Microsoft Security Response Center at http://www.microsoft.com/security/msrc/default.mspx .

[1] See Formation of Incident Response and Security Teams (FIRST), *A Complete Guide to the Common Vulnerability Scoring System Version 2.0.* http://www.first.org/cvss/cvss-guide.html

Other patches (such as application patches) are identified at the relevant vendor's site. The sites below are examples of these locations:

- Cisco- http://www.cisco.com/en/US/products/products_security_advisories_listing.html
- Juniper- http://www.juniper.net/support/security/

Information Security collates the provided list of relevant patches for discussion and review at the patch management committee. When other teams identify relevant patches, they will work with Information Security to document and analyze impact and necessary actions: including the determination of whether the patch is an immediate release or scheduled release patch. Patch management is a partnership where all interested and affected parties participate.

Evaluation Process

***All Microsoft security patches are automatically deemed to be patches that should be applied to workstations and servers*.** Systems Support and Server Support teams *should by default apply these patches without further evaluation from Information Security*. Once Systems and Server Support identify these patches, they should be moved into a testing process for further evaluation.

Non-Microsoft patches, with the exception of Cisco, will be rated by Information Security and passed back to the relevant BTS' teams such as Systems Support, Server Support and Corporate Applications team to take the necessary steps to evaluate the impact of these patches on their environments.[2] This evaluation process should include any backup and documentation necessary to roll back a patch deployment.

Functional teams that identify patches which negatively affect the performance and/or stability of a given environment are required to document this impact as well as suggest alternative solutions to mitigate the security risk posed by the lack of this security patch. Exceptions to patch deployments for those Microsoft patches with a "critical" rating or non-Microsoft patches with a rating of "7" or higher shall not be granted without the Information Security Manager's approval.

Deployment Process

Successfully evaluated patches shall be deployed according to the above listed schedule. Functional teams, such as OSS and Server Support, shall work with customers to identify any post deployment issues and document those for the Patch Management committee.

The table below identifies the method and deployment system utilizes for BTS's patch management system.

	Patch Identification System	**Patch Deployment System**	**Responsible Team/Division**
Network Devices			
-Routers/Switches	Web Search of Cisco Website	Manual	Networking
-Access Points	Web Search of Cisco Website	Manual	Networking
-Load Balancers	Web Search of F5 Website	Manual	Corporate Applications
-Security	Web Search of Tipping Point,	Manual	Information Security

[2] Cisco Systems creates a CVSS rating for their vulnerabilities and patches.

	Juniper, RSA Website		
Workstations	Windows Security Response Center	Altiris	Systems Support
Servers	Windows Server Update Services (WSUS)	Windows Server Update Services (WSUS)	Server Support

Revision History

Version	Effective Date	Authored By	Approved By	Date
1.0	3/31/09	Logan Kleier, Information Security Manager	BTS Leadership Team	3/13/09