

Security: Application & Maintenance of Patching Updates

Template

Contents

[**1** **INTRODUCTION** 3](#_Toc112955995)

[**2** **PURPOSE and Scope** 3](#_Toc112955996)

[**3** **AUDIENCE** 3](#_Toc112955997)

[**4** **GOALS & OBJECTIVES** 3](#_Toc112955998)

[**5** **KEY WORDS** 3](#_Toc112955999)

[**6** **DOCUMENTATION** 3](#_Toc112956000)

[**7** **PATCH MANAGEMENT PROCESS** 4](#_Toc112956001)

[**8** **PATCH MANAGEMENT LICENSING** 4](#_Toc112956002)

[**9** **MONITORING PRE-REQUIREMENTS FOR PATCH INSTALLATIONS** 4](#_Toc112956003)

[**10** **BASELINE INVENTORY** 4](#_Toc112956004)

[**11** **PATCH REVIEW LIST** 4](#_Toc112956005)

[**12** **PATCH PER ASSET REVIEW** 5](#_Toc112956006)

[**13** **MISSING PATCHES** 5](#_Toc112956007)

[**14** **ASSET LIST TABLE** 5](#_Toc112956008)

[**15** **PATCH CLASSIFICATION & DEFINITION** 5](#_Toc112956009)

[**16** **PATCH MANAGEMENT POLICIES** 6](#_Toc112956010)

[**17** **CHANGE MANAGEMENT** 6](#_Toc112956011)

[**18** **DEPLOYING APPROVED PATCHES** 6](#_Toc112956012)

[**19** **PREVENTATIVE MAINTENANCE SCHEDULES** 7](#_Toc112956013)

[**20** **SERVICE INTERRUPTIONS** 7](#_Toc112956014)

[**20.1** **ASSET MAINTENANCE GROUPS** 7](#_Toc112956015)

[**21** **COMMUNICATIONS PLAN** 8](#_Toc112956016)

[**22** **SECURITY RISKS** 8](#_Toc112956017)

[**22.1** **Risk Responses** 8](#_Toc112956018)

[**22.2** **Vulnerability Mitigation** 9](#_Toc112956019)

[**22.3** **Cyber Security Consideration** 9](#_Toc112956020)

[**23** **APPENDIX A: INCIDENT RESPONSE CHECKLIST** 10](#_Toc112956021)

# **INTRODUCTION**

{This template is design to assist in the application and management of patch updates. insert relevant introductions for your project}

# **PURPOSE and Scope**

{This section identifies the specific purpose and scope of the project. insert scope information for your project Example: The purpose and Scope of this document is to help USC IT organizations improve their enterprise patch management planning to strengthen the management of risk}

# **AUDIENCE**

{insert primary audience for this project Example: The primary audience for this template are Chief Information Officers, Chief Information Security Officers, Cybersecurity Directors, and Managers, including others who are responsible for managing organizational risk related to patch installations and updates}

# **GOALS & OBJECTIVES**

{This section identifies the goals and objectives of the project. insert general goals and objectives for your project}

# **KEY WORDS**

{insert table with key words and definitions utilized in this template

Sample: Patch management, Risk, Update, Upgrade, Vulnerability, Management, Accept, Mitigate, Transfer, Avoid}

# **DOCUMENTATION**

{insert table with a list of relevant documentation associated with this project}

# **PATCH MANAGEMENT PROCESS**

 {insert patch management process deliverables for your project. Consider a plan for each category listed below (if applicable)} Sample:

1. Create a Baseline inventory
2. Standardized software versions
3. Categorize by risk and priority
4. Set up test lab environment
5. Test patches
6. Gather Patch vulnerability and test information
7. Identify endpoints
8. Review this patch management plan
9. Run a pilot
10. Document both pre and post patching status

# **PATCH MANAGEMENT LICENSING**

{This section identifies the licensing requirements for deploying patches. Each asset must have a current license for updates – except in the case of in-house developed assets.

insert table, list, or chart displaying each asset and the license agreement for your project

# **MONITORING PRE-REQUIREMENTS FOR PATCH INSTALLATIONS**

*{This section identifies the minimum requirements for asset upgrades insert table, list, or chart displaying each asset and the minimum requirements for your project} Sample:*

|  |
| --- |
| **Asset Requirements** |
| **Component** | **Minimum Requirements** | **Recommended** |
| Computer and processor | 2.0GHz | Quad-Core Xeon or equivalent |
| RAM | 4 GB | 8 GB |
| HD Space | 16 GB | 32 GB |
| Display resolution | 1280x1024 display or above |  |
| Operating system (x64) | * Windows Server 2008 R2
* Linux
 | Windows Server 2012 and above (Servers 2016 and 2019 are supported) |

# **BASELINE INVENTORY**

{This section identifies an inventory list of all production systems, applications/software, Severs.

 insert table, list, or chart of all production systems including operating systems and applications for your project}

# **PATCH REVIEW LIST**

{This section identifies a list of required patches for application/software security. It also lists approved patches, failed patches, installed, and missing patches. insert table, list, or chart displaying each asset on the list for your project} Sample:

|  |
| --- |
| **Approved Patch List** |
| Patch Name | Security Bulletin | Details | Product | Classification | Type | Published | # Installed | Failed | Total Missing | App Owner  |
| 2445227 | n/a | Security update | Windows | Security | Important | 8/5/22 | 129 | 3 | 12 |   |
| 2874425 | n/a | Windows 10 | Unix | Service Packs | Mandatory | 8/7/22 | 15 | 2 | 7 |   |

# **PATCH PER ASSET REVIEW**

{This section identifies each approved patch per asset.

insert table, list, or chart displaying each patch per asset for your project}

# **MISSING PATCHES**

{This section identifies each missing patch not part of the license installation approved patch per asset. insert table, list, or chart displaying each missing patch for follow up or explanation for your project

# **ASSET LIST TABLE**

{This section identifies each asset on the list requiring patch updates and the required details.

insert table, list, or chart displaying each asset on the list for your project Sample:

|  |  |  |
| --- | --- | --- |
| **Default Asset List** |  |  |
| Asset ID | Name | Source | IP Address | Serial # | MFGR | Disabled | Storage Capacity |  Type | OS Name |  OS | Location |
| Acer-2 | CB802 | Agent | 10.14…. | 45892 | Acer | No | 0 GB | Workstation | Chrome | Chrome | USC |
| Dell-7 | C8701 | Manual | 192…….. | 89451 | Dell | No | 932 GB | Laptop | Chrome | Chrome | SF |
| VMWare | NB01 | Manual | 10.14….. | 22587 | Acer | No | 120 GB | Server | Win 10 | Win 10 | SEA |
| Citrix | SATB1 | Agent | 192…… | 78921 | HP | No | 238 GB | Server | Win 10 | Win 10 | USC |
| Unit | Dell9 | Agent | 192….. | 29581 | Apple | No | 170 GB | Workstation | Chrome | Chrome | Ireland |

# **PATCH CLASSIFICATION & DEFINITION**

 {insert table, list, or chart displaying each patch type and related definitions Sample: [this sample is for Microsoft Patch Classifications only]}

:

|  |
| --- |
| **Microsoft Patch Classification Definitions** |
| Critical Updates | A broadly released fix for a specific problem addressing a critical, non-security related bug. |
| Feature Packs | New product functionality that is first distributed outside the context of a product release, and usually included in the next full product release. |
| Security Updates | A broadly released fix for a product-specific security-related vulnerability. Security vulnerabilities are rated based on their severity which is indicated in the Microsoft security bulletin as critical, important, moderate, or low. |
| Service Packs | A tested, cumulative set of all hotfixes, security updates, critical updates, and updates, as well as additional fixes for problems found internally since the release of the product. Service packs may also contain a limited number of customer-requested design changes or features. |
| Update Rollups | A tested, cumulative set of hotfixes, security updates, critical updates, and updates packaged together for easy deployment. A rollup generally targets a specific area, such as security, or a component of a product, such as Internet Information Services "IIS". |
| *Updates*  | *A broadly released fix for a specific problem addressing a non-critical, non-security-related bug.* |

# **PATCH MANAGEMENT POLICIES**

{This section identifies the policies your organization have either created or is following to manage patch installations/updates. insert patch management policy for your project} Sample:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Last Scan/Time** | **Next Scan/Time** | **Latch Patch/Time** | **Next Patch/Time** | **Attached assets** |
| Server default policy | 08-02-2022 17:05 | 09-02-2022 18:12 | 05-12-202213:00 | 09-15-202213:00 |  |
| Workstation Default Policy | 08-02-2022 17:05 | 09-02-2022 18:12 | 05-12-202213:00 | 09-15-202213:00 |  |

# ***CHANGE MANAGEMENT***

*{This section identifies selected patches approved by Change Management for selected assets.*

*insert patch management policy for your project} Sample*

|  |
| --- |
| **Change Management Approval** |
| **Change Method** | **Asset** | **Patch** | **Approval** |
|  |  |  |  |
|  |  |  |  |

# **DEPLOYING APPROVED PATCHES**

{This section identifies the types of deployment for selected patches

insert method, list, or process used for deploying and consider the following types of deployment} Sample

* Schedule Automatic Patch Deployment
* Manually run policy patch
* Manually deploy patches
* Verify Deployment

# **PREVENTATIVE MAINTENANCE SCHEDULES**

{This section identifies the preventative maintenance schedules for patch installations and application security insert method, or process for developing a maintenance schedule for your project} Sample:

|  |
| --- |
| **Preventative Maintenance Schedule** |
| **Resource** | **Reason/Use** | **Start** | **End** |
| Admin Applications | System Maintenance | Wednesdays @ 1700 | Wednesdays @ 2300 |
| **Advanced Interactive Servers (AIX)** | **Extended Preventative Maintenance**Recycle of Individual Servers split between the Second and Third Sunday of February, May, August, November | Sundays - 0030 | Sundays - 0730 |
| **USC Cloud** | **Security Patches and Reboots** | Fridays - 1900 | Saturdays - 0600 |
| **Enterprise Linux Service - ELSGC1 Box (IML)** | **System Maintenance/IML**First Sunday of September, October, and November 20202 Includes the following LPARs: ZLX3, ZLX4, ZLX9 | Sundays - 2300 | Mondays - 0145 |
| **Network - 2022** | **2022 Network Normal PMs** | Sundays - 0400 | Sundays - 0700 |

# **SERVICE INTERRUPTIONS**

{This section identifies potential service interruptions due to patch upgrades

insert method, or process for a plan to mitigate potential interruptions for your project. Consider the following options: Sample

* Test all patch upgrades in the lab prior to deployment
* Utilize failover systems for immediate rollovers
* *Apply critical patches during non-business hours.*

## **ASSET MAINTENANCE GROUPS**

{insert method, list, or process for assigning each asset to a maintenance group to mitigate potential interruptions for your project. Consider the following options: Sample

|  |  |
| --- | --- |
| **Asset** | **Coverage Areas** |
| Mobile workforce laptops for standard end users | * Software to patch: Firmware, operating systems, and client applications for end user devices
* Outage restrictions: Tolerant to downtime
* Existing mitigations: Endpoint security controls running on the laptops
* Level of impact to the organization if compromised: Moderate
 |
| On-premises datacenter | * Software to patch: Firmware, operating systems, and applications for server platforms
* Outage restrictions: Must adhere to scheduled outage windows for all non-emergency situations
* Existing mitigations: Network-based security controls restricting access to the assets and security controls running on the assets themselves
* Level of impact to the organization if compromised: High
 |
| Legacy OT asset | * Software to patch: None; existing software is no longer supported and cannot be patched
* Outage restrictions: Must adhere to scheduled outage windows for all non-emergency situations
* Existing mitigations: Network isolation, physical security controls
* Level of impact to the organization if compromised: High
 |
| Smartphones for the mobile workforce | * Software to patch: Operating systems and mobile apps
* Outage restrictions: Tolerant to downtime
* Existing mitigations: Mobile device security controls running on the smartphones

Level of impact to the organization if compromised: Moderate |
| On-premises servers for automated software testing | * Software to patch: Firmware, server operating systems, virtualization software, server and client guest operating systems, server and client applications
* Outage restrictions: Usually tolerant to downtime
* Existing mitigations: Network-based security controls restricting access to the assets, and security controls running on the assets themselves
* Level of impact to the organization if compromised: Moderate
 |
| Containers with customer-facing applications in the public cloud | * Software to patch: Container operating systems, application modules
* Outage restrictions: Highly tolerant to downtime
* Existing mitigations: Security controls running on the container operating system
* Level of impact to the organization if compromised: High
 |

# **COMMUNICATIONS PLAN**

{This section identifies a communications plan to notify users of scheduled critical systems upgrades. insert method, or process for a communications plan to inform users of critical updates and potential for failures}. Sample

# **SECURITY RISKS**

{This section identifies any potential risks. insert method, table, or process to capture potential vulnerabilities. Categorize each asset by risk and priority, then create a vulnerability list to prioritize what need to be remediated quickly}

## **Risk Responses**

|  |
| --- |
| **Risk Responses** |
| Accept | Accept the risk from vulnerable software as is, such as by relying on existing security controls to prevent vulnerability exploitation or by determining that the potential impact is low enough that no additional action is needed |
| Mitigate | Reduce the risk by eliminating the vulnerabilities (e.g., patching the vulnerable software, disabling a vulnerable feature, or upgrading to a newer software version without the vulnerabilities) and/or deploying additional security controls to reduce vulnerability exploitation (e.g., using firewalls and network segmentation to isolate vulnerable assets, thus reducing the attack surface) |
| Transfer | Reduce the risk by sharing some of the consequences with another party, such as by purchasing cybersecurity insurance or by replacing conventional software installations with software-as-a-service (SaaS) usage where the SaaS vendor/managed service provider takes care of patching. |
| Avoid  | Ensure that the risk does not occur by eliminating the attack surface, such as by uninstalling the vulnerable software, decommissioning assets with the vulnerabilities, or disabling computing capabilities in assets that can function without them |

## **Vulnerability Mitigation**

{This section identifies any vulnerabilities for potential risks. insert method, table, or process to capture potential vulnerabilities and Risk mitigations} Sample:

|  |  |
| --- | --- |
| **Vulnerability Importance** | **Asset Importance** |
| **Low** | **Moderate** | **High** |
| **Low** | By deadline: 64.7 % Average time: 80.4 days Median time: 75.2 days | By deadline: 72.4 % Average time: 34.7 days Median time: 33.7 days | By deadline: 85.0 % Average time: 14.6 days Median time: 8.1 days |
| **Medium** | By deadline: 66.5 % Average time: 75.1 days Median time: 70.7 days | By deadline: 68.7 % Average time: 33.2 days Median time: 31.6 days | By deadline: 71.4 % Average time: 12.9 days Median time: 10.5 days |
| **High** | By deadline: 68.6 % Average time: 62.1 days Median time: 58.0 days | By deadline: 78.8 % Average time: 26.8 days Median time: 22.1 days | By deadline: 85.5 % Average time: 8.8 days Median time: 8.1 days |
| **Critical** | By deadline: 81.4 % Average time: 44.4 days Median time: 41.3 days | By deadline: 92.3 % Average time: 21.2 days Median time: 23.9 days | By deadline: 95.2 % Average time: 5.2 days Median time: 5.1 days |

## **Cyber Security Consideration**

{This section identifies any vulnerabilities relating to cyber security issues during patch upgrades. insert method, table, list, or process to capture potential cyber security issues vulnerabilities and Risk mitigations} Sample list:

|  |
| --- |
| **Cyber Security Risk Identification and Mitigation** |
| **Identification** | **Vulnerability Present** | **Report to Maintenance Team(s)** | **Mitigation**  | **Report Incident**  | **Continue Patching** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# **APPENDIX A: INCIDENT RESPONSE CHECKLIST**

{This Appendix is the incident response playbook for incidents that involve confirmed malicious cyber activity for which a major incident has been declared or not yet been reasonably ruled out. insert method, table, list, or process to capture Cyber Security incidents in real time}: Sample Table:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  **Step** | **Incident Response Procedure** | **Action Taken** | **Contact**  | **Date Completed** |
| **Step 1: Declare Incident**  |
| a | Perform initial categorization of incident |  |  |  |
| b | Notify Maintenance Team Leader. |  |  |  |
| c | Notify USC Campus Security and, if applicable, law enforcement. |  |  |  |
| **Step 2: Determine Scope of Investigation** |
| a | Identify the type and extent of the incident |  |  |  |
| b | Assess operational or informational impact on organization’s mission |  |  |  |
| **Step 3: Collect and Preserve Data** |
| a | Collect and preserve the data necessary for incident verification, categorization, prioritization, mitigation, reporting, attribution, and as potential evidence |  |  |  |
| b | Log all evidence and note how the evidence was acquired, when it was acquired, and who acquired the evidence. |  |  |  |
| **Step 4: Perform Technical Analysis** |
| a | Develop a technical and contextual understanding of the incident |  |  |  |
| b | Based on analysis thus far and available information form a hypothesis of what the adversary was attempting to access/accomplish |  |  |  |
| *c* | *Update scope as investigation progresses and information evolves. Report most recent findings and incident status to Maintenance Team Leader and USC Campus Security*  |  |  |  |
| *d* | ***Terminating condition:*** *Technical analysis is complete when the incident has been verified, the scope has been determined, the method(s) of persistent access to the network has/have been identified, the impact has been assessed, a hypothesis for the narrative of exploitation has been cultivated and all stakeholders are proceeding with a common operating picture.* |  |  |  |
| *e* | *Analyze logs to correlate events and adversary activity* |  |  |  |
| *f* | *Establish an incident timeline that records events, description of events, date-time group of occurrences, impacts, and data sources. Keep updated with all relevant findings*  |  |  |  |
| ***Identify Anomalous Activity*** |
| *g* | *Assess affected systems and networks for subtleties of adversary behavior which often may look legitimate.* |  |  |  |
| *h* | *Identify deviations from established baseline activity - particularly important to identify attempts to leverage legitimate credentials and native capabilities and tools (i.e., living off the land techniques)* |  |  |  |
| ***Identify Root Cause and Enabling Conditions*** |
| *i* | *Attempt to identify the root cause of the incident and collect threat information that can be used in further searches and inform subsequent response efforts.* |  |  |  |
| *j* | *Identify and document the conditions that enabled the adversary to access and operate within the environment.* |  |  |  |
| *k* | *Assess networks and systems for changes that may have been made to either evade defenses or facilitate persistent access.* |  |  |  |
| *l* | *Identify attack vector. This includes how the adversary accessing the environment (e.g., malware, RDP, VPN).* |  |  |  |
| *m* | *Assess (depth and breadth). This includes All compromised systems, users, services, and networks.* |  |  |  |
| ***Gather Incident Indicators*** |
| *n* | *Review available database for precedent of similar activity* |  |  |  |
| *o* | *Analyze adversary tools. Assess tools to extract IOCs for short-term containment* |  |  |  |
| *p* | *Identify and document indicators that can be used for correlative analysis on the network.* |  |  |  |
| *q* | *Share extracted threat information (atomic, computed, and behavioral indicators, context, and countermeasures) with internal response teams and CISA* |  |  |  |