

System Patching Policy

# Overview/Purpose

**<Utility Name>** is responsible for ensuring the confidentiality, integrity, and availability of its data and that of customer data stored on its systems. **<Utility Name>** has an obligation to provide appropriate protection against malware threats, such as viruses, Trojans, and worms which could adversely affect the security of the systems or data stored on the systems. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems within this scope.

This document describes **<Utility Name>**’s requirements for maintaining up-to-date operating system security patches on all owned and managed workstations and servers.

# Scope

This policy applies to the following equipment, systems, and applications owned or used by **<Utility Name>**:

* Computers - servers and workstations (including laptops)
* Mobile devices – smartphones, tablets
* Network equipment – firewalls, routers, switches, network protocol converters
* Software applications

# Policy

Computers, mobile devices, network equipment, and software applications owned or used by **<Utility Name>** must have up-to-date (as defined by <**person or group responsible for policy at Utility**> minimum baseline standards) system patches installed to protect the asset from known vulnerabilities. This includes updating applications, operating systems and firmware as required**.** Patching priority is adjusted according to severity level of the vulnerability which the patch addresses.

## Patching Priority

Patch management must be prioritized based on the severity of the vulnerability the patch addresses. In most cases, severity ratings are based on the Common Vulnerability Scoring System (CVSS). *See more information about CVSS in the Glossary section.*

A CVSS score of 7-10 is considered a Priority 1 vulnerability, a CVSS score of 4-6.9 is considered a Priority 2 vulnerability and a CVSS of 0.1-3.9 is considered a Priority 3.

|  |  |  |
| --- | --- | --- |
| Priority | CVSS Score | Patching Completion |
| 1 | 7 - 10 | Max 2 weeks |
| 2 | 4 – 6.9 | Max 4 weeks |
| 3 | 0.1 – 3.9 | Next patching cycle (3-6 months) |
| 4 | 0 | Discretionary |

IT Manager can assign Priority 1 to a vulnerability if the vendor has issued an emergency patch (CVSS might be not published yet) or other information indicate high probability of exploitation.

## Workstations

Desktops, laptops, and tablets must have automatic updates enabled for operating system patches, where available. This will be the default configuration for all workstations built by **<Utility Name>**. As possible, all software applications installed on workstations will be set to download and install patches automatically. Any exception to the policy must be documented and forwarded to the <**person or group responsible for policy** > for review. See Section 4.2 on Exceptions.

## Servers

Servers must comply with the minimum baseline requirements that have been approved by the <**person or group responsible for policy** >. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the **<Utility Name>** server and the data that resides on it. Any exception to the policy must be documented and forwarded to the <**person or group responsible for policy** > for review.

## Roles and responsibilities

IT Manager shall use the *Systems Patching Form* to assign responsibility for patching:

* Unix/Linux servers on the network,
* Microsoft Windows servers on the network,
* Workstations on the network,
* Applications.

IT Manager is responsible for routinely assessing compliance with the patching policy and will provide guidance to all groups in issues of security and patch management.

The System Patching Form is also used for:

* Approving emergency patches (no CVSS score),
* Reporting applied patches   
  (if reports are not collected by log management system).

## Monitoring and reporting

Active patching teams noted in Section 3.3 are required to compile and maintain reporting metrics that summarize the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk. These reports shall be made available to Information Security and Internal Audit personnel upon request.

# Compliance

## Compliance Measurement

The <**person or group responsible for policy** > will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved by the <**person or group responsible for policy** > in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with **<Utility Name>** HR policies.

# Related Standards, Policies, and Processes

* Adapted from “Cyber Security Policy Framework” (<https://www.nreca.coop/wp-content/uploads/2015/09/cyber_security_policy_framework.docx>)   
  Cyber Security Policy Framework was created by the Kentucky Association of Electric Cooperatives (KAEC) Information Technology (IT) Association - Cyber Security Subcommittee.
* PCI DSS Requirements (<https://www.pcisecuritystandards.org/document_library>)
* FIRST - Forum of Incident Response and Security Teams  
  Example of CVSS based Patching Policy  
  (<https://www.first.org/cvss/cvss-based-patch-policy.pdf>)

# Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible | Accountable | Consulted | Informed |
| IT Manager | **CEO/GM** | **IT Administrator** | **All Employees** |

*[Explanatory Note: <Utility Name> should feel free to alter section to reflect the specific responsibility requirement determined by <Utility Name> management.]*

# Approval

\_

<**Insert title of approver**> Date

# Revision History

|  |  |  |
| --- | --- | --- |
| Date of Change(s) | Revised by | Summary of Change(s) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |