COUNTY OF SAN MATEO

Virus, Patch, and Vulnerability Management Policy

Policy Update: 06/20/2017

Overview

Computer viruses are designed to exploit flaws or errors in software. These flaws or errors, known as vulnerabilities, can allow attackers the ability to gain access to and control a target computer which, in turn, becomes an entry point into the network. Desktops, laptops, servers, applications, and network devices can serve as access points to sensitive and confidential County data. Security updates, patches, and anti-malware software are used and implemented by ISD to protect and mitigate threats to the overall health of San Mateo County's network.

Policy Purpose

The purpose of this policy is to proactively manage San Mateo County's computing resources and prevent their infection by computer viruses and malicious code.

Scope

All users of the San Mateo County network, including parties who work on the computer or network systems, will be subject to the provisions of this policy. Contractors that are granted remote access by ISD/County shall be provided a copy of this policy and be required to agree to the content prior to being allowed access to County systems.

Policy

Virus Protection

A. All computers and fileservers connected to the San Mateo County network shall be configured in accordance with this policy as follows:
   1. All computer devices shall have the most recent version of anti-virus software that has been tested and approved by ISD, installed, and actively running on these devices.
   2. All computer devices shall be configured to automatically receive daily virus definition file updates from centrally administered resources managed by ISD.
   3. All files on computer devices shall be scanned periodically for viruses
   4. User shall not take action, without ISD approval, to exclude his or her computer from updates covered by this section.

B. An exception may be made by ISD in instances where the virus protection software interferes with a department's proprietary application processes and database structures. Prior to implementation of the nonconforming configuration, a waiver must be submitted to and signed by the Department Head responsible for the application/system and the Information Security Officer (ISO). All exceptions must be mitigated by other forms of protection and require.

Patch Management

A. ISD shall provide and maintain common software patches and updates for computing devices.
   1. All computers and fileservers connected to the San Mateo County network must be configured to receive updates and patches from the centrally administered resource.
   2. All patches shall be deployed by ISD within a reasonable time in relation to the level of risk. ISD shall prioritize that correct vulnerabilities that represent an imminent risk the County's computing environment. ISD shall adhere to the following prioritization guidelines:
      a. All updates categorized by the vendor as "critical" with known attacks shall be applied within 30 days of release.
      b. All updates categorized by the vendor as "critical" but with no known attacks shall be applied within 45 days of release.
      c. All updates categorized by the vendor as "important" shall be applied within 60 days of release.
      d. Non-security related patches, such as those that provide additional functionality or address performance issues, shall be completed as soon as adequate testing has been completed.
   3. If there is an active cyber incident, virus outbreak, or other critical issue that can be resolved with a security patch, ISD may direct its staff to immediately deploy a patch to all systems.
   4. All new devices shall be patched to the current level, as defined by the operating system vendor, prior to the device being connected to the County's network.
   5. If the County's centralized automated tool cannot be used for patching, the application owner must develop a process for provisioning updates and ensure updates are deployed.

B. Patch management on systems running proprietary applications may require vendor certification of patches prior to installation that includes consideration of the underlying operating system.
   1. In the event that a department requires an exception to a patch installation, any vulnerability shall be mitigated by other forms of compensating controls in consultation with ISD. The exception shall require an advance written waiver signed by the Department head responsible for the application/system and approved by the ISO.

Vulnerability Management

A. ISD shall periodically assess the security of the County's computer systems by conducting vulnerability assessments and penetration testing by scanning computing devices.
   1. Following these assessments, ISD shall recommend security fixes or other compensating controls to improve the security of the computing environment.

Computer Security Incident Response Team (CSIRT)

A. In the event of a threat to San Mateo County computing resources or a known exploit to an operating system is discovered, ISD shall work with the Countywide Computer Security Incident Response Team (CSIRT) to review and respond to computer security incident.

1. The CSIRT's roles and responsibility are as follows:
    a. The CSIRT shall consists of one representative from each County department or agency.
    b. The CIO or his/her designee shall act as the chair of the CSIRT.
    c. The CSIRT shall establish and maintain a communication mechanism for providing rapid and effective communication between team members.
    d. The CSIRT shall establish and maintain a formal virus alert system for notifying the County community of virus outbreaks and recommended measures.

B. Any system determined to be infected shall be quarantined and removed from the network. The system will not be allowed to return to the network until the infection has been eliminated.

Other County Policies

The County has other policies, including, but not limited to, the IT Security Policy and Remote Access Policy, that address specific areas of information security. Departments may also have internal policies relevant to the subject matter associated with the specific work of the department. In the event of a conflict, the policies providing the County with the greatest level of security will be applied.

Policy Enforcement

ISD retains the authority to disconnect an infected system from the network if the responsible Department fails to manage the infection in a timely manner. Any system found in violation of this policy could result in the system being taken offline until the situation has been corrected.

Revision History

Effective Date	Outcome
11/01/2004	Policy established
06/20/2017	Policy updated