

ATTACHMENT G

VULNERABILITY & PATCH MANAGEMENT STANDARD



City of Phoenix Enterprise Information Technology Standard

Domain: Information Security Operations			Number: 100-005	Title: Vulnerability & Patch Management Standard			
Authorizing A.R.: Authorizing Policy:			AR 1.84 - Information Security Management ISP-100-005 Vulnerability & Patch Management Policy				
Regulatory Framework			NIST: SP 800-53: IR-6, CM-8, CM-8(1), CM-8, PL-2, SA-4(1), SA-4(2), SR-12, PL-1, CM-2(3), CM-12, CM-12(1), PS-2, PS-9, PS-2, PS-3, PL-4, PL-4(1), PL-4, PS-6, PS-5, PS-7, IR-6, PL-2, SI-12, AC-21, PL-1, SA-2, CA-2, RA-9, RA-1, RA-2, RA-3, RA-7, SR-2, RA-3(1), SA-4, SR-1, RA-9, SR-2, SR-2(1), SR-5, SR-3, SA-9, SA-9(2), SR-6, SA-4, SI-5, AT-2(2).				
Original Approval			08/29/2022				
Number	Version	Pages	Effective Date	Last Review	Next Review	Approved by	Classification
2	1.1	5	08/29/2022	6/24/2024	6/24/2027	CIO/CISO	Internal

I. PURPOSE AND APPLICABILITY

The Vulnerability and Patch Management Standard describes the discovery, remediation, and ongoing monitoring of applications, systems, and environments to reduce the risk presented by technical vulnerabilities. The remediation of vulnerabilities within City systems, environments, and applications is standardized to ensure proper protection, reduce operational impacts, and ensure the overall security of City of Phoenix technology platforms.

This policy applies to City personnel with authorized access to City information and information systems. For this policy, the “City of Phoenix” is sometimes referred to as the “City.”

II. BACKGROUND

Vulnerability and Patch Management are critical components of the City’s information security program and are essential to help reduce its potential financial, reputational, and regulatory risks.

III. DEFINITIONS

For definitions of terms and acronyms, see the [ISG-000-003.1 Information Security Glossary](#). The following terms and acronyms are used in this standard:

1. Acunetix
2. Gytpol
3. Information Security Incident
4. ISO – Information Security Office
5. IT Assets
6. Mitigation
7. Patch
8. Patch Management
9. Penetration Testing

Domain: Information Security Operations	Number: ISS-100-005	Title: Vulnerability & Patch Management Standard
---	---------------------	--

10. Remediation
11. Risk
12. SOC – Security Operations Center
13. System Owner
14. Threat
15. Vulnerability Management
16. Vulnerability Management Team

IV. STANDARD

The Vulnerability and Patch Management Standard covers requirements, teams, monitoring and detection, vulnerability ranking, remediation, continuous monitoring, and post-remediation monitoring.

1. ISO Vulnerability Management Team

- 1.1. Through this standard, the City establishes a Vulnerability Management Team of specialized personnel responsible for managing vulnerabilities discovered on City systems.
- 1.2. The Vulnerability Management Team comprises members of the Security Operations Center (SOC) and the Information Security Office (ISO).
- 1.3. The Vulnerability Management Team will document formal vulnerability management standard operating procedures. This is required to protect the City's data and meet regulatory, contractual, and legal requirements.

2. Vulnerability Management Requirements

- 2.1. As ISO recommends, system owners shall adopt and implement all baseline and hardened configurations for all systems they operate, manage, or support.
- 2.2. As ISO requires, system owners are responsible for performing effective testing and following a consistent internal change management process for configuration changes.
- 2.3. All City systems, computers, and other devices must have up-to-date security patches as determined by the Vulnerability Management Team.
- 2.4. The Vulnerability Management Team will develop and implement a method for reviewing vendor and third-party security alerts against configuration standards and installed patches. The output of this process will be made available to ISO upon request.
- 2.5. System owners or their supporting staff must only turn off enterprise security controls by obtaining an approved exception per this standard.

3. Vulnerability Management Tools

- 3.1. The Vulnerability Management Team maintains various tools and a service approved by the CISO to conduct periodic vulnerability scans and assessments on City networks and systems.
- 3.2. Gypol - a Security Configuration Management platform the City of Phoenix deployed for automatic device hardening and repairing device misconfigurations.
 - 3.2.1. Provides continuous monitoring and automatic remediation caused by misconfigurations and non-compliance on endpoint devices.
 - 3.2.2. Gypol shall be deployed on all Windows, macOS, or Linux clients, servers, virtual machines, and cloud instances throughout the City.

- 3.3. Acunetix - a web application scanning tool ensures that all web applications developed, maintained, or used by the City of Phoenix are secure and compliant with industry best practices.
 - 3.3.1. Conducts web application vulnerability assessments, identifies and mitigates security vulnerabilities in web applications, and protects sensitive data to maintain the integrity and availability of web applications.
 - 3.3.2. All web applications and web services within the City of Phoenix, including production, development, and testing environments, must cover all application lifecycle stages, from initial development through deployment and maintenance.
 - 3.3.3. Scans should cover all aspects of the application, including but not limited to Input validation and output encoding (to prevent SQL Injection, Cross-Site Scripting, etc.)
- 4. Vulnerability Monitoring & Detection
 - 4.1. The Vulnerability Management Team conducts timely monthly vulnerability scans on all City departments.
 - 4.2. ISO will also conduct penetration testing on specific systems; similar remediation responsibilities apply to issues identified during penetration testing.
 - 4.3. If vulnerabilities are discovered, the SOC will send vulnerability reports to the CISO and alert system owners responsible for supporting devices and systems.
 - 4.4. The Vulnerability Management Team will conduct a vulnerability assessment:
 - 4.4.1. After the operating system installation.
 - 4.4.2. After the installation of any vendor-provided or in-house-developed application.
 - 4.4.3. Just before moving the IT Asset into production (if applicable).
 - 4.4.4. After an image or template is designed for the deployment of multiple devices.
 - 4.4.5. For vendor-provided information systems, before user acceptance testing and moving into production.
- 5. Vulnerability Ranking
 - 5.1. The City will rank and remediate vulnerabilities based on the rating of the NIST Common Vulnerability Scoring System (CVSS). Remediation must be prioritized based on the degree of associated severity and the impact on the confidentiality, integrity, or availability (C.I.A) of the vulnerable system.

Rating	CVSS Score
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

6. Remediation

- 6.1. Individuals responsible for supporting City devices and systems are expected to:
 - 6.1.1. Adhere to the remediation schedule defined by the Vulnerability Management Team.
 - 6.1.2. Mark false positives detected within the scanning console.
 - 6.1.3. Submit an exception request if a vulnerability cannot be remediated within the required timeframe or if remediation is deemed not technically feasible.
- 6.2. Suppose any identified vulnerability is believed to be a false positive or is otherwise believed to be not applicable. In that case, the following information is required to be concisely documented within the vulnerability scanning system and made available for CISO/ISO review:
 - 6.2.1. The affected system(s) and vulnerability.
 - 6.2.2. The plugin/service/software causing the false positive.
 - 6.2.3. Information/processes used to confirm that the vulnerability is, in fact, a false positive or otherwise not applicable.
- 6.3. System owners are responsible for ensuring vulnerability scans are not hindered by inadequate access to systems, applications, and devices. This will produce inaccurate and/or incomplete results.
 - 6.3.1. Authenticated scans shall be utilized to ensure that scans analyze the entire system and produce accurate and comprehensive results.
 - 6.3.2. With required access levels, scan results may produce 'false negative' results that accurately represent the system's security posture or device being scanned.
- 6.4. System owners or their support staff for individual systems must take steps to remediate these vulnerabilities.
- 6.5. System owners are responsible for following the patch management processes to apply operating system and application security patch updates for the IT systems, devices, and applications they manage.
- 6.6. All identified vulnerabilities that cannot be resolved must undergo a risk acceptance approval process.
- 6.7. Vulnerabilities are expected to be remediated within the following timeframes. The vulnerability management client will enumerate vulnerability severities. The timeframe to remediate a vulnerability will be calculated starting when both a scan has been completed, and a patch for the vulnerability has been released.
 - Critical vulnerabilities (9.0 - 10.0): 14 days
 - High vulnerabilities (7.0 - 8.9): 21 days
 - Medium vulnerabilities (4.0 - 6.9): 28 days
- 6.8. Once a patch is available from the vendor, the timelines are listed in 5.7. immediately apply.
- 6.9. More urgent remediation may be required in some instances (e.g., active exploitation on the city network or large-scale emerging threats actively leveraging exploits against city systems with critical and high vulnerabilities). The Vulnerability Management Team will alert system owners and define a specific timeframe for resolving these vulnerabilities. The CISO may also quarantine or disconnect any system or device from the City network.

Domain: Information Security Operations	Number: ISS-100-005	Title: Vulnerability & Patch Management Standard
---	---------------------	--

- 6.10. Departments and systems that handle sensitive data (e.g., data regulated by HIPAA, PCI, etc.) may be required to remediate vulnerabilities on a more expedited schedule, as required by contract, regulation, or law. System owners must be aware of whether such requirements apply to their systems.
- 6.11. If the CISO grants an exception request, compensating controls may be specified as part of the exception process. In most cases, exceptions are granted for a limited time (i.e., not permanent).
- 6.12. End-of-support systems (no longer being issued patches or security updates in response to vulnerabilities) must receive an exception approval or be replaced by a supported system.
- 7. Continuous Monitoring & Post Remediation Monitoring
 - 7.1. The City regards vulnerability and patch management as a continuous reoccurring process.
 - 7.2. Post-remediation monitoring will be conducted to ensure that the remediation steps taken were adequate to mitigate that vulnerability.

V. RELATED POLICIES, STANDARDS, AND PROCEDURES

Additional policies, IT standards, and procedures are developed to augment this policy as noted:

A.R. 1.69	Payment Card Industry Compliance Program
A.R. 1.84	Information Security Management
ISP-100-005	Vulnerability and Patch Management Policy
ISSOP-100-005.1	Vulnerability Management Internal PCI Scanning SOP
ISSOP-100-005.2	Vulnerability Management External ASV PCI Scanning SOP
(TBD)	EIS Patch Management Standard
NIST 800-53	Security Controls
NIST SP 800-40	Guide to Enterprise Patch Management Planning
	NIST Framework for Improving Critical Infrastructure Cybersecurity
	National Vulnerability Database
	Common Vulnerability Exposure Database


VI. QUESTIONS

Questions regarding this standard should be directed to the Information Security and Privacy Office by emailing ISO.Policy@phoenix.gov.

VII. APPROVAL

This Standard has been approved by:

Chief Information Security Officer


Shannon Lawson (Jun 24, 2024 11:16 PDT)

Shannon M. Lawson

Jun 24, 2024

Date

VIII. REVISION HISTORY

Version	Date	Detail of Changes
1.1	6/24/2024	Added new information/terms to cover Vulnerability Management Tools: Acunetix and Gypol.