| Queens College<br>Information Technology Standard | No: PR.DS.1.9 Patch Management |
|---|---|
| IT Standard:<br><br>**Patch Management** | Updated: 10/17/2022 |
| | Issued By: Office of the CISO<br><br>Owner: Information Technology Services |

## 1.0 Purpose and Benefits

Security patch management (patch management) is a practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization. By applying security related software or firmware updates (patches) to applicable IT systems, the expected result is reduced time and money spent dealing with exploits by reducing or eliminating the related vulnerability.

## 2.0 Authority

- **Responsible Office(s):** Information Technology Services
- **Responsible Executive(s)**: CIO
- **Responsible Officer(s)**: Chief Information Security Officer

## 3.0 Scope

This standard relates specifically to vulnerabilities that can be addressed by a software or firmware update (patch) and applies to all software used on the entity's systems. The Vulnerability Scanning Standard should be followed for requirements on addressing non-patched vulnerabilities.

## 4.0 Information Statement

1. Entities must assign an individual or group within IT operations to be responsible for patch management.

2. If patch management is outsourced, service level agreements must be in place that address the requirements of this standard and outline responsibilities for patching. If patching is the responsibility of the third party, entities must verify that the patches have been applied.

3. A process must be in place to manage patches. This process must include the following:

- monitoring security sources (Appendix A) for vulnerabilities, patch and non-patch remediation, and emerging threats;
- overseeing patch distribution, including verifying that a change control procedure is being followed;
- testing for stability and deploying patches; and
- using an automated centralized patch management distribution tool, whenever technically feasible, which:
    - maintains a database of patches;
    - deploys patches to endpoints; and
    - verifies installation of patches.

4. Appropriate separation of duties must exist so that the individual(s) verifying patch distribution is not the same individual(s) who is distributing the patches.

5. As per the Information Security Policy, all entities must maintain an inventory of hardware and software assets. Patch management must incorporate all installed IT assets.

6. 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). A CVSS score of 7-10 is considered a high impact vulnerability, a CVSS score of 4-6.9 is considered a moderate impact vulnerability and a CVSS of 0-3.9 is considered a low impact vulnerability.

7. To the extent possible, the patching process must follow the timeline contained in the table below:

| Impact/Severity | Patch Initiated | Patch Completed |
|---|---|---|
| High | Within **24 hours** of patch release | Within **1 month** of patch release |
| Medium | Within **1 week** of patch release | Within **2 month** of patch release |
| Low | Within **1 month** of patch release | Within **3 months** of patch release, unless ISO determines this to be an insignificant risk to the environment |

8. If patching cannot be completed in the timeframe listed in the table above, compensating controls must be put in place within the timeframes above and the exception process must be followed.

9. If a patch requires a reboot for installation, the reboot must occur within the timeframes outlined above.

## 5.0 Compliance

This standard shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the Chief Information Security Officer's exception process.

## 6.0 Definitions of Key Terms

This standard shall be subject to periodic review to ensure relevancy.

| Date | Description of Change | Reviewer |
|---|---|---|
| | | |

## 7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:
Chief Information Security Officer
Aaron Wheeler
Aaron Wheeler@qc.cuny.edu

## 8.0 Revision History

This standard shall be subject to periodic review to ensure relevancy.

| Date | Description of Change | Reviewer |
|---|---|---|
| 10/17/2022 | Initial Changes to apply to Queens College | DVogel |
| 03/20/25 | Added number convention and control title | AWheeler |
| | Policy Implemented | |

## 9.0 Related Documents

National Institute of Standards and Technology, Special Publication 800-40, Guide to Enterprise Patch Management Technologies

Common Vulnerability Scoring System

Vulnerability Scanning Standard

## Appendix A: SAMPLE SECURITY SOURCES FOR VULNERABILITY/PATCH/THREAT INFORMATION

- Vendor websites/notification lists
- Vulnerability Scanners
- Penetration Tests
- National Vulnerability Database