NATIONAL DATA
MANAGEMENT AUTHORITY

Patch Management Standard

Prepared By:

National Data Management Authority
March 2023

Document Status Sheet

	Signature	Date
Policy Coordinator (Cybersecurity)	**Muriana McPherson**	**31-03-2023**
General Manager (NDMA)	**Christopher Deen**	**31-03-2023**

Document History and Version Control

Date	Version	Description	Authorised By	Approved By
31-03-2023	**1.0**		**General Manager, NDMA**	**National ICT Advisor**

Summary

1. This standard establishes a practice to proactively prevent the exploitation of IT vulnerabilities.
2. It was adapted from NIST Cybersecurity Framework Policy Template Guide and SANS Institute.
3. This is a living document which will be updated annually or as required.
4. Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

1.0 Purpose

Security patch management (patch management) is a practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organisation. 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

The Permanent Secretary, Administrative Head, Head of Human Resources or their designated representative of the Public Sector Organisation is responsible for the implementation of this standard. For further information regarding the foregoing, please contact the Policy Coordinator - National Data Management Authority (NDMA).

3.0 Scope

This standard encompasses all systems, automated and manual, for which the Government of Guyana has administrative responsibility, including systems managed or hosted by third parties on behalf of the Government. It specifically addresses vulnerabilities that can be addressed by a software or firmware update (patch) and applies to all software used on the Government of Guyana's information systems. The Vulnerability Scanning Standard should be followed for requirements on addressing non-patched vulnerabilities. It is the user's responsibility to read and understand this standard and to conduct their activities in accordance with its terms.

4.0 Standard

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

4.2 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, organisations must verify that the patches have been applied.

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

4.3.1 monitoring security sources for vulnerabilities, patch and non-patch remediation, and emerging threats.

4.3.2 overseeing patch distribution, including verifying that a change control procedure is being followed;

4.3.3 testing for stability and deploying patches; and

4.3.4 using an automated centralised patch management distribution tool, whenever technically feasible, which:

4.3.4.1 maintains a database of patches;

4.3.4.2 deploys patches to endpoints; and
4.3.4.3 verifies installation of patches.

4.4 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.

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

4.6 Patch management must be prioritised 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.

4.7 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 week** of patch release
Medium	Within **1 week** of patch release	Within **1 month** of patch release
Low	Within **1 month** of patch release	Within **2 months** of patch release, unless ISO determines this to be an insignificant risk to the environment

4.8 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.

4.9 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 organisational policies and standards. Failure to comply with this standard may, at the full discretion of the Permanent Secretary, Administrative Head, or Head of Human Resources of the Public Sector Organisation, may result in the suspension of any or all privileges and further action may be taken by the Ministry of Public Service.

6.0 Exceptions

Requests for exceptions to this standard shall be reviewed by the Permanent Secretary, Administrative Head, Head of Human Resources of the Public Sector Organisation, or the Policy Coordinator NDMA. Departments requesting exceptions shall provide written

requests to the relevant personnel. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein.

7.0 Maintenance

The Policy Coordinator, NDMA shall be responsible for the maintenance of this standard.

8.0 Definitions of Key Terms

Term	Definition
Patch Management[1]	The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.
Patch[2]	A software component that, when installed, directly modifies files or device settings related to a different software component without changing the version number or release details for the related software component.
User[3]	Individual or (system) process authorized to access an information system.
Vulnerability[4]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

9.0 Contact Information

Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

[1] *Retrieved from*: NIST Information Technology Laboratory – Computer Security Resource Center https://csrc.nist.gov/glossary/term/patch_management
[2] *Retrieved from*: NIST Information Technology Laboratory – Computer Security Resource Center https://csrc.nist.gov/glossary/term/patch
[3] *Retrieved from*: NIST Information Technology Laboratory – Computer Security Resource Center https://csrc.nist.gov/glossary/term/user
[4] *Retrieved from:* NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/vulnerability