Vulnerability Management Policy

Information Technology

metergy™
SOLUTIONS

Effective as of March 25, 2021

Table of Contents

1. Policy Statement

This Vulnerability Management Policy (the "**Policy**") applies to Metergy Solutions Inc. and its subsidiaries (collectively, "**Metergy**").

The purposes of this Policy are to: (a) govern vulnerability management within the Metergy information technology network; (b) ensure that Metergy's technology assets are scanned for vulnerabilities and patched with the latest appropriate updates; and (c) to assist in maintaining secure and reliable information technology infrastructure.

2. Scope

This policy applies to all Metergy-provided mobile devices, computing devices, platforms and other technology.

3. Roles and Responsibilities

Metergy's information technology department (the "**IT Department**") is responsible for implementing this Policy and performing all actions contemplated therein.

4. Vulnerability Scans

4.1. Internal and external vulnerability assessments scans must be performed at least monthly and after any significant change in the corporate network (e.g. significant changes in firewall rules or upgrades to products within the environment).

4.2. Vulnerability reports will be delivered to the IT/application owners for remediation.

4.3. Vulnerability scan results of each month are to be documented and retained for review.

4.4. Vulnerability metric reports will be produced for the IT leadership team on a scheduled basis.

5. Scanning New Devices and Applications

5.1. When replacing or adding new devices (e.g. routers, switches and servers) or applications (e.g. new web applications or new connectivity software), a compliant vulnerability scan must be conducted prior to connection or implementation on any production network. The scan results and any documentation related to any remediation that took place must be retained.

6. Security Update and Patching

6.1. IT/application owners are responsible for timely patching of security updates.

6.2. All production systems on the Metergy information technology network must be patched for known vulnerabilities, including newly released systems software patches, bug fixes and upgrades.

6.3. All critical vulnerabilities must be mitigated within 45 days and high and medium vulnerabilities must be mitigated within 60 days.

6.4. Requests for exception of the time to patch requirement above may be requested in writing to the security team within the IT Department and will be evaluated to determine if mitigating controls can lower the risk to an acceptable level.

6.5. Security patches must be acquired only from vendors or other trusted sources. Security patches must be approved by the security team within the IT Department before installing. System administrators must verify the integrity of the security patch in a test environment, following documented test procedures, before application to ensure it will not cause any negative impact upon production systems.

7. Vulnerability Remediation

7.1. Remediation plans and reports of action taken will be maintained by the security team within the IT Department. Re-scans will be performed to verify remediation of critical and high-level vulnerabilities.

8. Penetration Testing

8.1. Penetration testing will be performed at least annually by an accredited 3rd party company and in accordance with paragraph 5.2 of NIST Special Publication 800-115, dated September, 2008 (available at: https://csrc.nist.gov/publications/detail/sp/800-115/final) ("**NIST SP 800-115**"). Penetration testing will be conducted using the 4 phases of planning, discover, attack and reporting, as detailed in paragraph 5.2.1 of the NIST SP 800-115.

8.2. All external IP addresses that could be used to gain access to the corporate network must be tested.

8.3. Noted exploitable vulnerabilities found are to be corrected and testing repeated to confirm the correction.

9. Critical Levels

9.1. Criticality levels can be defined using the Common Vulnerability Scoring System ("**CVSS**"), where applicable. Vulnerabilities not listed with a CVSS score will be assigned a criticality level by the security team within the IT Department. The CVSS is an open framework scoring system for communicating the characteristics and severity of software vulnerabilities (available at: https://nvd.nist.gov/vuln-metrics/cvss).

9.2. Criticality levels will be adjusted by the IT Department, dependent on mitigating controls that may include authentication and authorization, network segmentation, encryption and others.