METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY # INFORMATION SECURITY POLICY	POLICY NUMBER: 19
SUBJECT: VULNERABILITY DISCLOSURE	DISTRIBUTION DATE: 10/6/2021
	EFFECTIVE DATE: 10/6/2021
ISSUING AUTHORITY: DIRECTOR OF INFORMATION TECHNOLOGY SERVICES OF T HE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY	EXPIRATION: UNTIL RESCINDED

PURPOSE

The purpose of this policy is to help the Metropolitan Government of Nashville and Davidson County (Metropolitan Government) improve its security posture by giving security researchers clear guidelines for conducting vulnerability discovery activities and to convey processes in how to submit discovered vulnerabilities to Metropolitan Government.

This policy describes what systems and types of research are covered under this policy, how to submit vulnerability reports, and how long the Metropolitan Government asks security researchers to wait before publicly disclosing vulnerabilities.

The Metropolitan Government encourages contacting us to report potential vulnerabilities in our systems.

POLICY

1.0 Authorization

If security researchers make a good faith effort to comply with this policy during security research, the Metropolitan Government of Nashville and Davidson County (Metropolitan Government) will consider the research to be authorized, will work with the security researcher to understand and resolve the issue quickly, and Metropolitan Government will not recommend or pursue legal action related to the research. Should legal action be initiated by a third party against the security researcher for activities that were conducted in accordance with this policy, Metropolitan Government will make this authorization known.

2.0 Guidelines

Under this policy, “research” means activities in which the security researcher:

- Notifies the Metropolitan Government as soon as possible after the discovery of a real or potential security issue.
- Makes every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only uses exploits to the extent necessary to confirm a vulnerability’s presence. Does not use an exploit to compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems.
- Provides the Metropolitan Government a reasonable, mutually agreed to amount of time to resolve the issue before the finding is disclosed publicly.

- Does not submit a high volume of low--quality reports.

Once the security researcher has established that a vulnerability exists or encounters any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), the security researcher must stop the test, notify the Metropolitan Government immediately, and not disclose this data to anyone else.

3.0 Test Methods Not Allowed

- Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data.
- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non--technical vulnerability testing.

4.0 Scope

This policy applies to the following systems and services**: *.nashville.gov**

Any service not expressly listed above, such as any connected services, are excluded from scope and are not authorized for testing. Additionally, vulnerabilities found in systems from Metropolitan Government vendors fall outside of this policy's scope and should be reported directly to the vendor according to their disclosure policy (if any). If you aren't sure whether a system is in scope or not, contact us at metroitshelpdesk@nashville.gov before starting your research.

Though the Metropolitan Government develops and maintains other internet--accessible systems or services, active research and testing must only be conducted on the systems and services covered by the scope of this document. If there is a particular system not in scope that the security researcher thinks merits testing, please contact the Metropolitan Government to discuss it first.

5.0 Reporting a Vulnerability

Information submitted under this policy will be used for defensive purposes only — to mitigate or remediate vulnerabilities. If findings include newly discovered vulnerabilities that affect users of a product or service and not solely the Metropolitan Government, Metropolitan Government may share the report with the Cybersecurity and Infrastructure Security Agency, where it will be handled under their coordinated vulnerability disclosure process. Metropolitan Government will not share name or contact information without express permission.

Metropolitan Government accepts vulnerability reports via metroitshelpdesk@nashville.gov . Reports may be submitted anonymously. If contact information is shared, the Metropolitan Government will acknowledge receipt of the report within 10 business days.

By submitting a vulnerability, the security researcher acknowledges that there is no expectation of payment and expressly waives any future pay claims against the Metropolitan Government related to the submission. In order to help triage and prioritize submissions, please include the following in the report:

- Describe the location the vulnerability was discovered and the potential impact of exploitation.

- Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).
- Be in English, if possible.

If contact information is shared, the Metropolitan Government commits to coordinating as openly and as quickly as possible.

- Within 5 business days, Metropolitan Government will acknowledge that the report has been received.
- Metropolitan Government will provide confirmation that issue has either been addressed or risk has been reported to applicable department and agency.

SCOPE, BACKGROUND and GOVERNANCE

This information is set forth in the *Metropolitan Government Scope, Background and Governance Statement for Information Security Policies*.

DEFINITIONS

Terms used in this policy are defined in the Metropolitan Government Information Security Glossary.

CONTACT

Questions should be directed to (615) 862-6222 or by email at ciso@nashville.gov

SIGNATURE

Keith Durbin
Chief Information Officer/Director of ITS
Metropolitan Government of Nashville and Davidson County

REFERENCES

- Binding Operational Directive (BOD) 20-01
- General Services Administration's Technology Transformation Services' VDP
- Department of Defense's VDP
- Framework for a Vulnerability Disclosure Program for Online Systems
- VDP template from a 2016 working group of the National Telecommunications and information Administration
- International Organization for Standardization, ISO/IEC 29147:2014
- NIST Special Publication 800-171 rev. 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*
- NIST Cybersecurity Framework ver. 2.0

REVISION HISTORY

REVISION	DATE	CHANGES

1.0	10/6/2021	Original Version
1.1	8/29/205	Change to reflect use of rev 2 of NIST Cybersecurity Framework Change to reflect use of NIST 800-171 r3 as a reference