POLICY

VULNERABILITY DISCLOSURE

POL-208

The City of Seattle is committed to ensuring the security of the public's data by protecting their information. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our preferences in how to submit discovered vulnerabilities to us.

This policy describes **what systems and types of research** are covered under this policy, **how to send us** vulnerability reports, and **how long** we ask security researchers to wait before publicly disclosing vulnerabilities. This policy is meant specifically for individuals who are not City staff.

We encourage you to contact us to report potential vulnerabilities in our systems.

Scope

This policy applies to the following systems and services:

- *.seattle.gov
    - Hosted on 156.74.248.0/21

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 our 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 security@seattle.gov before starting your research.

Test Authorization

If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized, we will work with you to understand and resolve the issue quickly, and the City of Seattle will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this policy, we will make this authorization known.

Though we develop and maintain other internet-accessible systems or services, we ask that active research and testing 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 you think merits testing, please contact us to discuss it first. We will increase the scope of this policy over time.

Test Conditions

Under this policy, "research" means activities in which you:

- Notify us as soon as possible after you discover a real or potential security issue.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.

- Only use exploits to the extent necessary to confirm a vulnerability's presence. Do not use an exploit to compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems.
- Provide notification ninety (90) days before you disclose it publicly. We may request an extension depending on the complexity of the vulnerability or permit disclosure sooner if patch is available sooner.
- Do not submit a high volume of low-quality reports.

Once you've established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), **you must stop your test, notify us immediately, and not disclose this data to anyone else**.

Test methods

The following test methods are not authorized:

- 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
- Scanners, scrapers, or automated tools which produce excessive amounts of traffic.

Reporting a vulnerability

Information submitted under this policy will be used for defensive purposes only – to mitigate or remediate vulnerabilities. If your findings include newly discovered vulnerabilities that affect all users of a product or service and not solely City of Seattle, we may share your report with the vendor. We will not share your name or contact information without express permission.

We accept vulnerability reports at security@seattle.gov Reports may be submitted anonymously. If you share contact information, we will acknowledge receipt of your report within three (3) business days.

What we would like to see from you

In order to help us triage and prioritize submissions, we recommend that your reports:

- 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).

What you can expect from us

When you choose to share your contact information with us, we commit to coordinating with you as openly and as quickly as possible.

- Within three (3) business days, we will acknowledge that your report has been received.

- To the best of our ability, we will confirm the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution.
- We will maintain an open dialogue to discuss issues.

Questions

Questions regarding this policy may be sent to security@seattle.gov. We also invite you to contact us with suggestions for improving this policy.

Version	Content	Approver:	Approval Date
v 2.0	Issuance and Provisional Approval	Greg Smith, Chief Information Security Officer	**12/3/2022**
	Final Approval	**Jim Loter, Interim Chief Technology Officer**	**12/3/2022**

Jim Loter (Dec 22, 2022 08:25 PST)