Reporters MUST adhere to the following guidelines.

1 General

- Reporters MUST comply with all applicable laws and regulations in connection with security research activities or other participation in this vulnerability disclosure program.
- Reporters MUST abide by all Gems Setra Terms of Service(s).
- Reporters SHOULD make a good faith effort to notify and work directly with the affected vendor(s) or service providers prior to publicly disclosing vulnerability reports.

2 Scope of Authorized Testing

- Reporters MAY ONLY test Gems Setra hardware and software sold to customers with the explicit written permission of that customer (“Authorized Equipment”), to detect a vulnerability for the sole purpose of providing Gems Setra information about that vulnerability. “Authorized Equipment” does not include the Gems Setra web sites and properties.
- Reporters SHOULD only test against test accounts owned by the Reporter or with explicit written permission from the account holder if they abide by the Terms of Service for that account.
- Reporters MUST avoid any harm to Gems Setra's information systems, products, and customers.
- Reporters SHOULD contact Gems Setra at psirt@gemssetra.com if at any point you are uncertain of whether to proceed with testing.

3 Coordination with Gems Setra

- Reporters SHOULD submit vulnerability reports, including any Gems Setra websites and properties to Gems Setra by email at psirt@gemssetra.com.
- Reporters SHOULD submit high-quality reports that contain sufficient descriptive details to permit Gems Setra to reproduce the vulnerable behavior accurately.
- Reporters SHOULD NOT report unanalyzed crash dumps or fuzzer output unless accompanied by a sufficiently detailed explanation of how they represent a security vulnerability.
- Reporters MAY include a proof-of-concept exploit if available.
- Reporters MAY request that their contact information be withheld from any affected vendor(s) outside of Gems Setra.
- Reporters MAY request not to be named in the acknowledgments of Gems Setra's public disclosures.
- Reporters MUST NOT require Gems Setra to enter a customer relationship, non-disclosure agreement (NDA) or any other contractual or financial obligation as a condition of receiving or coordinating vulnerability reports.
- Gems Setra SHALL confirm receipt of the vulnerability report with the Reporter.
- Gems Setra MAY investigate the vulnerability report and inform the reporter through the means defined in the report submission.
- Gems Setra MAY contact the vulnerability reporter for more information if Gems Setra cannot validate the reported vulnerability.
- Gems Setra MAY communicate with the vulnerability reporter on the mitigation status.
- Gems Setra MAY communicate with the vulnerability reporter when a mitigation has been validated and when it will be released to Gems Setra customers.
- Gems Setra MAY attribute the vulnerability reporter in any security advisories Gems Setra publishes about the vulnerability the reporter discovered. The vulnerability reporter will have the option to opt-out of being attributed, at reporter’s discretion.
- GEMS SETRA RESERVES THE RIGHT TO DEVIATE FROM THESE GUIDELINES IN SPECIFIC INSTANCES.

4 Coordination with Vendors

- If the Reporter finds a vulnerability in a Gems Setra hardware or software product due to a vulnerability in a generally available product or service, the Reporter MAY report the vulnerability to the affected vendor(s),

service provider(s), or third-party vulnerability coordination service(s) to enable the product or service to be fixed.

5 Coordination with Others

- Reporters SHOULD NOT disclose any details of any Gems Setra hardware or software vulnerability or any indicators of vulnerability to any third party.

6 Public Disclosure

- Reporters MAY disclose to the public the prior existence of vulnerabilities already fixed by Gems Setra, including potential details of the vulnerability, indicators of vulnerability, or the nature (but not the specific content) of information rendered available by the vulnerability.
- Reporters choosing to disclose to the public SHOULD do so in prior consultation with Gems Setra.
- Reporters MUST NOT disclose any incidental proprietary data revealed during testing.

7 Safe Harbor

- When a Reporter conducts security research and reports a vulnerability in good faith and in accordance with this policy, Gems Setra will consider those activities authorized and will not initiate legal action against the Reporter solely for those activities.
- If a third party initiates legal action against a Reporter for activities that Gems Setra determines were conducted in accordance with this policy, Gems Setra MAY make known that the Reporter’s activities were conducted in compliance with this policy.
- This safe harbor does not authorize violations of applicable law, access to third-party systems or data without permission, privacy violations, service disruption, extortion, threats, or activities outside the Scope of Authorized Testing.
- Reporters remain responsible for complying with applicable law. If a Reporter is uncertain whether planned testing is permitted, the Reporter SHOULD contact psirt@gemssetra.com before proceeding.