maximus

Good Faith Security Research

All vulnerability research must be conducted in good faith

This means:

- You will follow this policy, and any other relevant agreements you have with us
- Your research must consist exclusively of good faith testing, investigation, or correction of a security flaw, with the primary goal of promoting the safety of the class of devices, machines, or online services to which any accessed computers belong
- You will not violate Maximus customers' security and privacy, and will not harm individuals or the public
- Your research will proceed only as far as necessary to demonstrate or clarify the security issue, and no further
- If a vulnerability provides unintended access to data, you will limit the amount of data you access to the minimum required for effectively demonstrating a proof of concept. Stop the research and submit a report immediately if you encounter any user data during testing, such as personal information, financial information, or proprietary information
- You will report the findings of your research to us within 72 hours of determining a potential security concern via our Vulnerability Disclosure Program
- You will provide us with a reasonable amount of time to resolve the issue before you disclose it publicly
- You may only interact with accounts you own or with explicit written permission from Maximus or the account owner
- No stunt hacking
- No extortion or harassment

Safe Harbor

We consider Good Faith Security Research to be authorized activity that is protected from adversarial legal action by us. This means that for activities conducted in accordance with this policy, while the program is active, we:

- **Will not** bring legal action against you or report you for Good Faith Security Research, including for bypassing technological measures we use to protect the applications in scope.

Note that for the purposes of safe harbor, Maximus does **NOT** waive a right to pursue remedies against security research activities targeting other Maximus customers' resources, operations, or end users, including but not limited to:

- Unauthorized cross-customer environment access
- Manipulation, monitoring/collection
- Spoofing
- Social engineering, including but not limited to phishing
- Impersonating Maximus, Maximus employees, Maximus services, or Maximus offerings
- Impersonating Maximus or customer marketplace offerings (eg., AMIs, container images, templates, models, etc)
- Impersonating any other company, their employees, services, products or offerings
- Provisioning resources to mimic Maximus infrastructure or Maximus customer resources
- Denial of Service, Distributed Denial of Service, simulated DoS, simulated DDoS
- Port, protocol, or request flooding
- Any type of brute forcing
- IP or Resource cycling/churning
- DNS hijacking, Pharming, or zone walking

An explicit authorization or permission granted by any single Maximus customer for the purposes of their continuous vulnerability scanning, penetration testing, security configuration validation, or vulnerability rewards program (VRP) cannot exceed the bounds of the specific customers' accounts and resources and does NOT grant authorization for abusive activities.

Individuals or companies conducting security research are strongly encouraged to contact Maximus Security to review their planned methodology and seek guidance or operational support prior to any activities. Security research that Maximus determines has not been conducted in good faith may subject your Maximus account(s) to active response measures, such as offending resource isolation, account suspension, resource / account termination, legal remedies, or relevant law enforcement referral.

Keep in mind that we are not able to authorize security research on third-party infrastructure, and a third party is not bound by this safe harbor statement.