# MageHost B.V. | Responsible disclosure

January 2021

We pay great attention to the safety and integrity of our systems and services. Nevertheless, a weak spot, vulnerability, exploit or other security risk (hereinafter referred to as: 'security risk') may still be discovered.

We ask that you report any security risks you have identified to us as soon as possible, with due observance of the following policy. This will enable us to continuously improve the security of our systems and services and to continue to strive to offer our clients and users the most secure experience possible.

**For this purpose, we ask that:**

1. in investigating the matter:
    - you do not use distributed denial of service attacks (DDoS);
    - you do not make use of brutal force attacks;
    - you do not post malware;
    - you do not use phishing and/or hacking tools;
    - you do not make changes to systems or the data stored therein;
    - you do not use social engineering or attack physical security measures;
    - you do not use spam;
2. in investigating the matter, you do not go beyond what is strictly required to share the security risks with us in accordance with this policy and do not take advantage of these by – for example – accessing third-party data, overloading systems or creating a nuisance to users of the systems in any other way;
3. you report the security risks and all your related findings in an [info@magehost.pro], containing, to the extent possible:
    - as clear a description of the security risk as possible;
    - the IP address or URL of the relevant system; and
    - a clear description of the steps that will enable us to reproduce and/or establish the finding;
4. you keep your findings strictly confidential and do not share them with others until the relevant security risk has been remedied; and
5. you delete any confidential information that has come into your possession as a result of the investigation as soon as the relevant security risk has been remedied.

**You may expect us to:**

1. not attach any legal consequences to your report, provided that, in investigating and reporting your findings, you followed the procedure described in this policy;
2. treat all reports confidentially and not share your personal data with third parties without permission, unless we are required to do so by law or pursuant to a court ruling;
3. – if you wish, and insofar as there is going to be a public or other communication or publication on the security risk – mention you as the person who discovered the security risk (please note that it is possible that someone else has discovered the security risk first, without that being disclosed at the time. In such case, the other party will be considered the party who discovered it.);

4. respond to your report with our assessment of your findings and an expected solution date within seven days;
5. make every effort to resolve the security risk and keep you informed of the progress with regard to the solution; and
6. – in principle – be open to contributing to any publications on your findings after the security risk has been remedied.

We offer no rewards for reporting security risks.