

# K-Master - Disclosure Policy

## 1. Responsible disclosure policy

We consider security and data protection of our customer a top priority. To this aim, we adopt a secure development process of our systems, services and applications, but we cannot totally avoid vulnerabilities. The Responsible Disclosure Policy describes how to notify us a vulnerability and the behaviour we ask a customer, researcher or expert that should identify one or more vulnerabilities in order to help us to further improve our levels of security and reliability and better protect our customers and their data. Telepass reserves the right to update the present policy at any time. Personal data will be processed in accordance with our [privacy policy](#).

## 2. Scope

Whenever a customer, researcher or expert should identify one or more vulnerabilities in the following environments:

- Mobile applications bearing the KMaster logo and published on official stores:
  - Telepass KMaster
- KMaster portals:
  - telepasskmaster.com
  - partner.telepasskmaster.com
  - selftest.telepasskmaster.com

## 3. Responsible disclosure

- E-mail your findings to [security@telepass.com](mailto:security@telepass.com);
- Encrypt your findings using our PGP key to prevent this critical information from falling into the wrong hands;
- [PGP Key](#) - Fingerprint: B426 E58E CE47 9503 9CBC 17F5 0669 7574 1042 4A7F
- Do not take advantage of the vulnerability or problem you have discovered;
- Do not perform any activity that can damage us or our users, disrupt the impacted system or service or cause any data leakage/loss;
- Make every effort to avoid breaches of privacy, deterioration or suspension of services and destruction of data;
- Respect the privacy of our users and/or customers: you are not allowed to use any personal data for purposes other than protect our users and their data, in accordance with this policy.
- Do not make changes to the system or application;
- Do not use Denial of Service attacks or brute force access;
- Do not use aggressive automated scanning;
- Do not use social engineering of our employees or contractors;
- Do not use attacks on physical security;
- Do not place a backdoor in a system. By placing a backdoor in a system, that system becomes even more insecure;
- Do provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible. Usually, the IP address or the URL of the affected system and a description of the vulnerability will be sufficient, but complex vulnerabilities may require further explanation;
- Do not reveal the problem to others until it has been resolved and in any case before sharing with us the contents that you intend to disclose;
- Maintain a responsible attitude even after the patch release, carefully evaluating the type of information released and always with the purposes of preserving our users and their data.

#### **4. KMaster commitment**

- We will respond to the report within 7 business days with our evaluation of the report and an expected resolution date;
- We will not take any legal action against who discovers and reports security breaches in compliance with this Responsible Disclosure Policy,
- We will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission, unless it is necessary to comply with a legal obligation. Reporting under a pseudonym or anonymous is possible;
- We will keep you informed of the progress towards resolving the problem;
- In the public information concerning the problem reported, we will give your name as the discoverer of the problem (unless you desire otherwise);
- As of now, we do not offer bounties for valid submissions,
- In our public responsible disclosure informational page, we will report your name as the discoverer of a problem (unless you desire otherwise) to recognize your precious contribution to our and our customer information security.

We reserve the right not to manage and act against reports and discovers that do not respect the criteria indicated in our Responsible Disclosure Policy and into the applicable laws.