HiPay

# Vulnerability Disclosure Policy

ENGLISH

# Introduction

At HiPay, we take the security of our products and services seriously. We recognize the importance of working with the security community to identify and address vulnerabilities in our systems.

This vulnerability disclosure policy details how ethical hackers can report potential security issues to us, and how we will respond to such reports.

# Reporting a vulnerability

If you discover a potential vulnerability in our products or services, we encourage you to report it to us as soon as possible. Please send an email to soc@hipay.com, providing as much detail as possible about the vulnerability, the affected system or service, tools and scripts used in the discovery process and how it can be reproduced.

We request that you do not publicly disclose the vulnerability until we have a chance to investigate and address it.

Avoid exploiting the vulnerability beyond what is necessary to demonstrate its existence.

Do not modify or delete data that does not belong to you.

# Test methods

The following test methods are not authorized :

- Network denial of service (DoS or DDoS) tests or other tests that impact a service, damage a system or damage data.
- Physical testing (office access, open doors, tailgating etc...)
- Social engineering (all types of phishing) or any other non-technical vulnerability testing
- Tests that involve unauthorized access to our servers

# Scope

This policy applies to the following domain names :

- *.hipay.com

- *.hipay-tpp.com

Any service not explicitly listed above, such as any connected services, are excluded from scope and are not authorized for testing.

# Hall of Fame

For the moment we don't give financial rewards.

We maintain a public Hall of Fame to recognize individuals who report valid security issues to us. If you would like to be included in our Hall of Fame, please let us know when you report the vulnerability.

We will not take legal action against individuals who act in good faith and follow this policy when reporting security vulnerabilities to us. We also commit to protecting the confidentiality of your personal information to the extent possible, and to not sharing your personal information with third parties without your consent, unless required by law.