Fraud and Abuse Policy 2015
Contents

4. Introduction
6. Policy Goal
7. Combatting Customer Fraud and Abuse
8. Reporting Breaches
9. How Alleged Breaches Will Be Investigated
10. Abuse
13. Fraud
14. Working with the Police, National Crime Agency (NCA) and other government agencies
15. Reporting Procedures
16. Overview
HEG conducts its business in a legal and ethical manner which is upheld strongly by the Code of Conduct in its communication and demonstration of the behavior that is required from employees, individuals and organisations which we partner with.

Therefore, when faced with risks from wrong doing, HEG aims to create a rigorous anti-fraud and anti-abuse culture that promotes honesty, integrity, openness and vigilance. Creating and embedding such a culture requires support from internal departments and customers to help discover, report and document such acts.

HEG understands that the internet does not recognize geographical or legal boundaries and neither do cybercriminals. However, with over 1.7 million HEG customers based around the world, who use a wide range of our services, it is impossible to monitor each and every site a customer manages or hosts with us.

All HEG customers are required to comply with their respective brand’s acceptable use policy.
2. Policy Goal

With the abuse of online services having grown rapidly we all face a number of Fraud and Abuse related threats on a daily basis. HEG faces threats such as:

- Malicious users regularly seeking to abuse the services we provide to our customers;
- Customers using our services in an abusive way; and
- Customers attempting to fraudulently purchase services from us.

Fraud and Abuse of our services can have a significant negative impact on HEG, our customers and society as a whole. This can include but is not limited to; interruption of service for customers, unwelcome sexual, violent and hateful content, unauthorised information disclosure, financial loss and reputational damage.

This policy has been produced by HEG to help customers understand the threat from fraud and abuse and communicate the basic procedures HEG have in place to help manage and mitigate the associated risks. For the avoidance of doubt, this policy is non-contractual.

This policy can be found at heg.com.
3. Combatting Customer Fraud and Abuse

HEG works to minimise the amount of Fraud and Abuse that is generated on its servers. We have dedicated Fraud and Abuse teams “the Team” across a number of our offices that work hard to minimise the impact associated with customer Fraud and Abuse and investigate cases involving but not limited to:

- Spam and spam-vertising;
- Services running vulnerable software;
- Port scanning, attempted hacking and firewall activity;
- Child abuse;
- Malware; and
- Malicious activity.
3.1 Reporting Breaches

All reports of abuse are investigated and customer facing policies expressly state that customers are prohibited from providing the following services:

- Spam;
- Hacking attempts;
- IRC activity;
- Phishing;
- Peer to Peer online exchanging;
- Anonymisation services;
- Content abuse;
- Suspected terrorism; and
- DDOS.

Each HEG brand has its own local Acceptable Use Policy (AUP) which communicates prohibited material and actions, outlining the consequences of breaching the AUP. HEG customers are contractually required to comply with the AUP at all times and failure to do so may lead to termination of the services to that customer.

Therefore, HEG encourages its customers to read through HEG’s Abuse and Acceptable Use Policies when encountering something that they think might constitute an abuse and reporting any abuse they spot which they believe has come from any of the HEG brands’ networks.

Suspected abuse can be reported by email to abuse@[hegbrand].com | de | es | uk or to abuse@heg.com, when in doubt.
3.2 How Alleged Breaches Will Be Investigated

While the action taken by the Team depends on the product it relates to, all issues brought to the attention of HEG are investigated thoroughly; relevant customers are contacted and we work to resolve the issue as quickly as possible.

Depending on the circumstances HEG reserves the right to:

• Immediately suspend the customer’s access;
• Immediately end the customer’s relevant HEG contract;
• Notify and/or pass on the details of the breach to any relevant government statutory, self-regulatory or law enforcement authority; and
• Remove (permanently) data or other material on HEG’s network and/or servers.

Investigations are carried out in accordance with local laws and regulations and the preservation of confidentiality in criminal cases is vital to ensure evidential security.

For more detail on how HEG handle contentious issues please see below.
3.3 Abuse

The following applies to all Abuse matters at HEG and outlines how such matters will be dealt with.

3.3.1 Spam and spam-vertising

The transmission of spam whether or not via HEG servers or services, is not tolerated. Our Fraud and Abuse team fully investigate all allegations of spam and take the appropriate action to resolve the matter.

HEG defines spam as the sending of irrelevant and unsolicited messages. This can include but is not limited to, the following:

- Email Messages
- Windows system messages
- Pop-up messages (aka “adware” or “spyware” messages)
- Instant messages (using AOL, MSN, Yahoo or other instant messenger programs)
- Online chat room advertisements
- Guestbook or website forum postings
- Facsimile solicitations
- Text/SMS messages

For spam complaints the Team would normally permit customers reasonable time to respond and confirm reasonable steps have been taken to address the issue or at least that the matter is being investigated.

In cases where there is immediate or imminent risk to multiple customers, such as spam being sent from a compromised mailbox or website (including Malware and Phishing), HEG aims to take immediate action to stop the activity. This could be disabling a mailbox or if no other choice available, suspending the entire account, including website and all email addresses if this is the only action left to us for the account type.

Pre-emptive checks are carried out by HEG to pro-actively identify any mailbox which may be being used for spamming. This includes daily monitoring of email logs and offending accounts and suspending them to minimize the impact on other customers.

3.3.2 Services Running Vulnerable Software

Customers are required to keep software updated. A failure to maintain up-to-date software in the environment is one of the primary causes of compromised services in the hosting space. For unmanaged services HEG endeavors to notify the affected customer.
3.3.3 Malicious Network Activity

HEG is aware that compromised servers are often used to attack external parties. This can include attempts to brute force login to other sites or scanning servers for vulnerabilities. Such activities can include port scanning, hacking and botnet activity. Customers are contacted when we receive notification of this activity. Where we deem there is a severe impact on our networks, we may immediately suspend the server. In all other cases, we allow customers the opportunity to respond and confirm with us that reasonable steps have been taken, to address the issue.

3.3.4 Malware

Web sites are also often hacked to host malicious content which can include virus or phishing sites. When we are made aware, we immediately suspend the site and notify the customers of the actions taken. Once we receive a response from the customer, we assist them in resolving the issue before the site is put back online.

3.3.5 Child Abuse

Any child exploitation and related abuse content that is reported to HEG will be immediately reported to the police.

3.3.6 Intellectual Property and Defamation

HEG will respond to any alleged breaches and always co-operate with any agency or rights holder wishing to assert their right. This can include but is not limited to, the following:

- Use of Trade Mark or Copyrighted text/ images on a website including distribution of copyrighted content, such as movies, via any means, including peer to peer file sharing protocols such as Bit Torrent;
- Passing Off (Appearing to impersonate another business, intentional or otherwise);
- Takedown requests (From government agencies, police / SOCA etc.); and
- Defamation (material that may damage another party’s reputation including but not limited to revenge videos/pictures, drawings, posts etc.).
3.3 Abuse

Complaints relating to Intellectual property matters or defamation are handled in a similar manner to complaints of abuse, in that we also permit customers the chance to respond. Where the customer fails to make appropriate changes to resolve the allegation within a reasonable timeframe we will take any reasonable steps to take the alleged infringing material offline. For example, this may involve suspending a shared hosting account using the support tool or requesting the relevant technical support team to suspend the website, on a VPS or Dedicated Server.

In the event that we discover a customer is continuing to breach our policies despite being warned and re-offends, we reserve the right to refuse, cancel or suspend their services at our sole discretion.

3.3.7 Suspected Terrorism

HEG liaise with government authorities in relation to servers, accounts and customers who are generally suspected of engaging in terrorist related activity.
3.4 Fraud

Fraud in the context of this policy is in regards to HEG customers using HEG services to facilitate fraud therefore, methods to decrease motive are difficult for HEG to address.

However, HEG is keen on restricting opportunity by way of taking action immediately and training staff on fraud awareness to develop their skills in detecting it in the first instance.

In support of this we have developed our own specialist in-house Fraud Prevention System (FPS) which is able to score orders according to our own rules for signs of potential fraud and only hold payment and provisioning for those with a high risk of being fraudulent. This involves blacklisting IP addresses where necessary.
3.5 Working with the Police, National Crime Agency (NCA) and other government agencies

Any enquiries from law enforcement agencies should be sent to the appropriate address below:

behoerden@hosteurope.ch
behoerden@hosteurope.de
spoc@hosteurope.es
behoerden@plussserver.de
spoc@plussserver.com
behoerden@Server4You.de
spoc@Server4You.com
behoerden@serverloft.de
spoc@serverloft.com
spoc@unmetered.com
spoc@heartinternet.co.uk
spoc@sign-up.to
spoc@domainmonster.com
spoc@domainbox.com
spoc@heg.com
4. Reporting Procedures

Great care will be taken in the investigation of suspected improprieties or irregularities so as to avoid mistaken accusations or alerting suspected individuals that an investigation is under way.

In line with industry practices, HEG report illegal activity to the police or to any other relevant authorities. We also work with all appropriate bodies to ensure illegal content is removed from our servers and reported as quickly as possible and suspected terrorist activity is reported via the relevant government channels, without delay.
4. Overview

HEG aims to achieve a reasonable balance between investigating fraudulent and abusive matters and providing a quality customer service.

Our System Administration team proactively monitors our infrastructure for any potentially abusive activity and work with the Fraud and Abuse Team to ensure customers are notified and own the incident through to completion.