ABUSE POLICY

Classification: Public

Version: 1.2

Contents

1 INTRODUCTION

This document describes the way in which Eurofiber handles abuse reports and counts as the Abuse policy.

1.1 What is abuse?

For Eurofiber, abuse means the abuse of services provided by Eurofiber to its customers. Eurofiber services may not be used for any action or operation contrary to the agreement with its customers, the law, public morals and public order. This is also stated in our contracts and terms and conditions. Creating abuse, not acting on abuse, or not acting timely to stop abuse by the customer is considered as not acting in accordance with the contractual agreements with Eurofiber.

Eurofiber also acknowledges that abuse is not always a conscious action of customers. Customer equipment may be infected with malware, which may, for example, cause it to unknowingly become part of a botnet and thus cause an abuse event to be detected and reported. Every party on the internet can report possible abuse to Internet service providers like Eurofiber. You can report Eurofiber abuse cases to abuse@eurofiber.com

Eurofiber therefore strives to timely inform the customers of possible abuse and will always try to support in resolving reports of possible abuse. It is however the customers' responsibility to act in accordance with the applicable laws and regulations.

1.1.1 Types of abuse

Abuse may occur in several different ways. Below are some examples. Please bear in mind that there may be other examples that can be flagged as abuse and therefor eligible for an abuse report, this list is therefore not exhaustive:

- Spam
- Phishing
- Port scanning
- Hacking
- Vulnerability scanning
- DOS/DDOS
- IP Spoofing
- Downloading and uploading illegal content
- Terrorism and child pornography hosting[1]
- Other illegal content hosting
- Deliberately altering the signal on the optic fiber line
- Deliberately altering the packets on the optic fiber line

If you are unsure whether an action is allowed on an Eurofiber line ask before you execute.

[1] This type of abuse requires extra attention due to European anti-terrorism legislation. See '1.2.2 *Measures*'

2 SCOPE DEFINITION

Eurofiber has a notifying role. When we receive a report from a third party about possible abuse, we will assess if the report is valid and if we need to inform our customers about the abuse. We will always inform a customer when the abuse falls in the categories mentioned in 1.1.1.

When we inform a customer about abuse, these notifications will be sent from our abuse mailbox: servicedesk@eurofiber.com. It is the responsibility of our Security Operation Center (SOC) to address abuse reports and adequately inform customers. Our SOC will also assist in troubleshooting the abuse notifications to the best of their ability. Our SOC will always create an incident ticket combined with the appropriate follow-up to both our customers as the Abuse reporter.

3 APPLICABILITY OF THE ABUSE POLICY

This policy applies to all Eurofiber group entities in the Netherlands and Belgium.

4 MEASURES

Depending on the type of abuse and the extent to which it occurs from a specific customer, the SOC will take appropriate actions to stop the abuse. Below are some examples of potential measures. Customers of Eurofiber who do not act accordingly can be held accountable by Eurofiber for actions originating from their acquired service

4.1 Sending/distributing Spam, phishing, DDOS and others

Eurofiber will inform and advise the customer to check the equipment for malware. An email will be sent to the technical contact person of the customer.

- **2nd report:** In the event of a second report on the same type of abuse, the SOC will send another email to the customer and additionally urge them to stop the abuse.
- **More than 2 reports:** The SOC will contact the technical contact person of the customer by phone to insist that the abuse must be stopped. The customer is given a 2 week notice to resolve the issues.
- **Notification after telephone contact:** When after 2 reports and contact via telephone the abuse persists and reports still come in, we reserve the right to take measures until the customer has proven that the abuse has been resolved.
- **In some extreme cases, Eurofiber may choose to first close the connection and then contact the customer.**
- Following the nature of the abuse and the applicable legal regulations Eurofiber might be obligated to report the abuse to the local authorities. Eurofiber reserves the right to inform the local authorities in any case of abuse.

4.2 Copyright complaints

Eurofiber strives to keep its network as transparent, open and free as possible. Eurofiber acknowledges that not all forms of abuse can be accepted, but we do not take any action regarding the enforcement of copyright complaints, unless we are legally obliged to do so.

Vulnerabilities on customer equipment

There are several parties that scan internet-accessible equipment for vulnerabilities. When an IP address that is owned by Eurofiber is scanned by this type of vulnerability scanning, Eurofiber receives a notification about this. Eurofiber will forward these notifications to the relevant customer for investigation. The customer is responsible for finding out and resolving the possible vulnerability. Our SOC will help to resolve the issue and can assist in the follow-up to the reporting party.

Terrorism material and child pornography hosting

It is mandatory under European law (Directive 2017/541) to take terrorism and child pornography material offline within hours of reporting such content. Eurofiber might receive a fine if this type of content is not taken offline within these time constraints. As a result, when a "Notice and Takedown" comes in regarding this type of content, we are forced to take immediate action. A customer failing to comply with these notice and take down requests might face the complete closure of their internet access.

The Eurofiber SOC is especially alert to incoming reports concerning this type of content. It will respond to these types of requests as quickly as possible. Terrorism material and child pornography hosting related reports have the highest priority in the context of abuse at all times.

4.3 Extreme cases

Eurofiber stands for an open and transparent network. Eurofiber therefore strives to behave according to this principle. In extreme cases in which the laws and regulations are not complied with, and or our standards and values are not respected and a customer does not comply with either the law or our standards, Eurofiber reserves the right to not engage with a potential customer, or to discontinue its services with an existing customer, if necessary in order to preserve the integrity and security of the network. This can also be the result of either a request from the judiciary, or may initiated by Eurofiber.

Examples of such extreme cases are:

- Bulletproof hosting
- Hosting illegal content
- Hosting services that are abused for illegal content

5 NOTICE AND TAKEDOWN

Eurofiber may receive official "Notice and Takedown" requests. These requests are focused on the removal of illegal content. Eurofiber is obliged to act on these requests.

If such a request is received, the standard process for “Notice and Takedown” will be started. Which encompasses at least the following steps:

- **Receive and Process the Notice**: Eurofiber will process the DMCA notice to determine if it is a legal request.
- **Remove Infringing Content**: If the notice is valid, Eurofiber will request the customer to expeditiously remove the allegedly infringing material.
- **Inform the Requester**: Notify the requester who posted the material that the Customer has removed the content because of their DMCA takedown notice.