Responsible Disclosure Policy

At Telenet we place great importance on the security of our systems and data. Despite the measures we take to optimize our security, it is nevertheless possible that something will slip through the net. Should you discover a security problem, we have a system in place for you to report it to us in a responsible way. We are happy to have your help to improve our systems and protect our customers even better.

This procedure is intended for reporting:

- Suspected vulnerabilities in our products and services, including modem, Digicorder/Digibox, hotspot/homespot, websites, web-based applications and mobile apps that can be abused and can lead to:
  - theft of sensitive data
  - unauthorized modification or deletion of sensitive data
  - interference with or prevention of access to our services
  - disruption of the proper operation of our network, products or services

This procedure is **not** intended for reporting:

- Questions or complaints about the operation of our products, services, invoicing, etc. Please contact our customer service department for matters of this type.
- DDoS attacks, brute force password guessing, social engineering attacks, etc.
- Notifications about viruses, phishing mail, spam mail, fraud, etc.

Guidelines

- Report the suspected vulnerability via the secure 'Report a security problem' page. Describe the problem in sufficient detail, and include the necessary evidence, such as IP addresses, log entries, screenshots, etc.
- Write your message in Dutch or English.
- If you prefer to remain anonymous, you are not required to provide us with contact information. However, in some cases we may want to reach you for further information or to provide feedback. One option that is open to you is to provide an anonymous mailbox (e.g. via Gmail or Hotmail).
- Only notify Telenet of your findings, and only via this procedure. Do not publish details about the security issue through other channels. Making the problem known through other channels or the media, even before or after notifying Telenet via this procedure and even when not all details are provided, will be considered irresponsible behaviour and can still lead to the filing of criminal charges.
- Do not exploit the identified leak: only collect the information necessary to demonstrate its existence.
- Do not change or delete any data or system settings.
- Handle any found data in a responsible manner: if you can demonstrate that there is a security problem with a small portion, do not go any further.

Responsible Disclosure Policy

Important!

Always operate within legal boundaries when identifying potential security issues. Do not demonstrate security vulnerabilities by performing DDoS attacks, brute force password guessing, social engineering activities, infecting systems with malware, scanning our systems, etc. Such actions will be considered and dealt with as targeted attacks, because they can cause harm to both Telenet and its customers. In such cases, Telenet cannot guarantee that you will not be prosecuted, since there is a risk that the authorities will take the necessary measures in response to such attacks.

Our promise

- We will respond to your message as soon as possible, if you have provided contact information.
- If we require additional information, we may choose to contact you, if possible.
- We will do everything possible to resolve any shortcomings as quickly as possible, and we will keep you posted.
- Depending on the potentially identified security problem, Telenet may autonomously decide to grant a reward. The content and scope of a reward will be unilaterally determined by Telenet, and any such reward may not be construed as a guarantee of future rewards.
- Acting in accordance with these guidelines ensures that Telenet will not file a criminal complaint against you.