WeTransfer Responsible Disclosure Policy

At WeTransfer we take great pride and care in designing our service in such a way that everyone can use it easily, safely and securely. Despite our efforts, we know that security vulnerabilities can never be fully prevented at all times. Security researchers and the internet community have an important role in keeping WeTransfer secure. For those who believe they have found a vulnerability in our service, we encourage them to act responsibly and report this vulnerability in accordance with this Responsible Disclosure Policy so we can work together to ensure the safety and security of our service and users.

This policy explains how to report a vulnerability, what the process is and how we will respond to such reports. We've made an effort to make this policy as easy and clear as possible, but do let us know if there are things you don't understand. You can contact us at secureforsure@wetransfer.com. If you think you've found a vulnerability in our security, we appreciate it if you do the right thing and make a responsible disclosure to us first.

Vulnerabilities
If you believe you have discovered a security vulnerability in the WeTransfer service, please send an email to secureforsure@wetransfer.com with a thorough explanation of the (characteristics of the) vulnerability (Authentication/Authorisation, CSS, CSRF, XML, SQL, etc.) and with sufficient details, including a Proof-of-Concept, which system or systems are concerned and how we can reproduce your steps.

How soon will we respond?
Depending on the vulnerability, our support team will reply as quickly as possible, or at least within 24 hours. Your report will then be quickly routed to the person best able to evaluate and act on your report. Someone from our staff will contact you personally to understand what the vulnerability is and to learn how we can patch it. You will receive a digitally signed confirmation of receipt of your report and how to contact your designated case handler to discuss the next steps. We will keep you updated on the progress during the process. If it is likely that the vulnerability has a larger impact on the ICT community than WeTransfer alone, we might also report the vulnerability to the National Cyber Security Center (NCSC, see www.nscs.nl).

Publishing the vulnerability
We do not publish information about specific vulnerabilities or reports we have received under this responsible disclosure policy. However, at your request, we can provide a personal reference on your request.

Recognition and remuneration
Anyone who is kind enough to report a significant vulnerability responsibly and follows the rules of this responsible disclosure policy, we will provide with WeTransfer memorabilia or a WeTransfer Plus account (with a value of $120). The reward may be based on the quality of the disclosure and nature of the vulnerability. If you prefer to make your report as John Doe (anonymously) or under a pseudonym, be our guest.

PGP public key
Please send us your report in an encrypted or digitally signed message.

What does not count as a vulnerability?
Although we appreciate your efforts, there are certain acts that do not count as a vulnerability that falls within the scope of this Responsible Disclosure Policy. This policy thus does not allow for:

- gaining access by ways of social engineering;

- creating your own back-door to gain access to the system. This could damage our service and create additional, unnecessary security risks; or
- DDoS or brute-force attacks.

Indemnification
WeTransfer will, within reason, hold blameless anyone who in good faith penetrates our site, and in the process of exploring or experimenting, extracts a small amount of sensitive data, as long as that person promptly notifies WeTransfer and destroys any data collected.

If you follow the rules of this responsible disclosure policy and act in good faith, WeTransfer will not take legal action against you or ask law enforcement to start criminal investigations. Not acting in good faith includes, but is not limited to:

- providing any information with regard to the vulnerability to any third party without the consent of WeTransfer;
- misusing the vulnerability in any way; or
- copying, deleting or altering any of the WeTransfer related data you have gained access to.

Legal action can be taken against disclosers of whom WeTransfer suspects that they did not act in good faith when penetrating the website or any related systems.

Questions?
If you have any questions regarding this Responsible Disclosure Policy, please do not hesitate to contact us by sending an e-mail to secureforsure@wetransfer.com.