RESPONSIBLE DISCLOSURE POLICY

SECURITY VULNERABILITY REPORTING

At Crossyn, the security of our platform is one of our top priorities. Despite our concern for the high degree of security, vulnerabilities may still become apparent after all.

Did you find a (possible) vulnerability within our system? Let us know! We would like to cooperate with you to further improve the security of our platform.

Would you like to report a security vulnerability? Please, send an e-mail to service@crossyn.com and provide:

- Your name;
- Your contact details;
- Your company name (if applicable) with each report.

We will investigate legitimate reports and make every effort to quickly correct any vulnerability. We promise you to:

- Confirm we received your report within 1 working day;
- Respond within 10 working days with our review of the report and a time planning for a solution;
- Award the first reporter an appropriate monetary reward, starting at 10 euro up to a maximum of 150 euro, for increasing the security of our platform and not take legal action against you or ask law enforcement to investigate you;
- The aforementioned reward is only applicable if it is deemed the reported issue is deemed a vulnerability that Crossyn is willing to act on and if the issue has to do with a Crossyn system.

If you comply with the following **Responsible Disclosure Guidelines:**

- Provide details of the vulnerability, including information needed to reproduce and validate the vulnerability;
- Handle carefully by not performing any other actions than those which are necessary to reveal the security problem;
- Agree to not resort to DDOS attacks or perform any social engineering on Crossyn employees;
- Avoid privacy violations, destruction of data and interruption or degradation of our services;
- Do not modify or access any data;
- Do not share or publish any information until the vulnerability is corrected.