e-contract.be
SAFE E-TRANSACTIONS

Responsible Disclosure

Policy

e-Contract.be BV
Brusselsesteenweg 30B
1652 Beersel
https://www.e-contract.be
info@e-contract.be

October 15, 2024
Version: 1.0.2
Classification: Public

1 Introduction

This Responsible Disclosure Policy is aimed at improving the performance and security of the services offered by e-Contract.be BV.

2 Policy scope

This target audience for this policy are all suppliers, vendors, customers, freelancers, employees related to e-Contract.be BV, all users of the e-Contract.be services, and everyone with good intentions to identify actual, potential or suspicions of vulnerabilities in the e-Contract.be services or potential performance improvements.

Our policy relates to security vulnerabilities that could be abused by third parties or interfere with the proper functioning of our products, services, network or IT systems.

The scope of products, services or websites of this policy is limited to those published on the company website www.e-contract.be.

For questions about the scope of this policy, please contact us at info@e-contract.be.

3 Policy

3.1 Access to systems

Access to the e-Contract.be BV systems that are covered by this policy is granted only to persons whose intention is to improve our systems or services security, to inform us of existing vulnerabilities, and that are in strict compliance with the other conditions set out in this policy.

Systems dependent on third parties are outside the scope of this policy, unless these third parties explicitly agree in advance to these rules.

3.2 Proportionality

Participants must comply strictly with the principle of proportionality in all their activities, i.e. never to disrupt the availability of the services provided by e-Contract.be BV and not to exploit vulnerabilities beyond what is strictly necessary to demonstrate the security issue.

Their approach must remain proportionate: if the security problem has been demonstrated on a small scale, no further action should be taken.

3.3 Prohibited actions

Participants are not permitted to take the following actions:

- copying or altering data from the IT system or deleting data from that system;
- changing the IT system parameters;
- installing malware: viruses, worms, Trojan horses, etc.;

- execute (Distributed) Denial of Service ((D)DOS) attacks;
- social engineering attacks;
- phishing attacks;
- spamming;
- stealing passwords or brute force attacks;
- installing a device to intercept, store or learn of (electronic) communications that are not accessible to the public;
- the intentional interception, storage or receipt of communications not accessible to the public or of electronic communications;
- the deliberate use, maintenance, communication or distribution of the content of non-public communications or of data from an IT system where the participant should reasonably have known it had been obtained unlawfully.

3.4 Confidentiality

Under no circumstances may participants share any information collected under this policy without our prior and express consent with third parties or disseminate this information to third parties.

Nor is it permitted to communicate IT data, communication data or personal data to third parties or to distribute this data to third parties.

Our policy is not intended to allow the deliberate disclosure of the content of IT data, communication data or personal data, and such disclosure may only occur by accident in the context of the detection of vulnerabilities.

If participants enlist assistance from a third party to perform their test, they shall ensure that the third party is aware of this policy in advance and agrees to comply with the terms of the policy, including confidentiality, when providing assistance.

3.5 Bona fide execution

e-Contract.be BV undertakes to implement this policy in good faith and not to bring civil or criminal proceedings against any participant who strictly complies with its terms and conditions and who has not intentionally caused harm to the IT systems concerned.

There can be no fraudulent intent, intent to harm, or desire to use or cause harm to the visited system or its data on the part of the participant.

In case participants are in doubt about certain conditions of our policy, they must consult e-Contract.be BV in advance and must act in accordance with the written answer they receive.

3.6 Processing of personal data

A coordinated disclosure policy is not intended to primarily and intentionally process personal data.

Unless it is necessary to prove the existence of a vulnerability, participants are not allowed to consult, retrieve or store personal data.

However, participants may, even by accident, get access to personal data that is stored, processed or transmitted in the IT system concerned.

It may also be necessary for the participant to temporarily consult, retrieve or use personal data in the context of vulnerability detection.

In this case, participants must notify e-Contract.be BV beforehand via info@e-contract.be.

When processing such data, participants undertake to comply with the legal obligations concerning the protection of personal data [1]and to comply with the terms of this policy.

The processing of personal data for purposes other than the detection of vulnerabilities in e-Contract.be BV's systems, equipment or products is not allowed.

Participants may not store any personal data processed for longer than is necessary. During this period, participants must ensure that this information is stored with a level of protection that is proportionate to the risks (preferably encrypted). After being used for the purpose of the policy, this data must be deleted immediately.

Finally, participants must inform us of any loss of personal data as soon as possible after becoming aware of it.

4 Reporting security vulnerabilities

4.1 Point of contact

The information discovered can be send to the following address:

e-Contract.be BV
Brusselsesteenweg 30B
1652 Beersel

email: info@e-contract.be
phone: +32 478 29 94 92

Communication can be done in Dutch or English.

4.2 Information to be provided

The following information should be provided:

- Your first and last name

[1] Regulation No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR).

- Your contact info (e.g. e-mail address or phone number)
- A description of the vulnerability
- The impacted service (name, IP address, server, ...)
- The type of vulnerability (remote access, information leak, ...)
- How to reproduce the vulnerability
- Logs showing the result of the vulnerability
- Tools used
- Exact date and time the vulnerabilities were tested or used
- Any relevant information (screenshots, proof of concept, ...)

5 Procedure

5.1 Notification

Participants undertake to notify e-Contract.be BV referred to in point 4.1 of this policy as soon as possible about information on any vulnerabilities.

After receiving a notification, e-Contract.be BV undertakes to send the participant a confirmation of receipt, within a reasonable period of time, containing its internal reference number, a reminder of the obligation of confidentiality and the next steps in the procedure.

If participants do not receive a confirmation of receipt within a reasonable period of time, they may contact e-Contract.be BV's Information Security Officer (infosec@e-contract.be) so this representative can contact e-Contract.be BV's technical team.

5.2 Communication

The parties undertake to do their utmost to ensure permanent and effective communication. After all, the information provided by participants may be very useful in identifying a vulnerability and resolving it.

5.3 Analysis

During the analysis phase, e-Contract.be BV will reproduce the environment and the vulnerability identified, to check the information provided.

e-Contract.be BV undertakes to keep participants regularly informed of the results of its analysis and of the action taken based on their notification.

In the course of this program, parties are required to link to similar or related notifications, assess the risk and severity of the vulnerability and to identify any other affected products or systems.

5.4 Developing a solution

The goal of this policy is to enable the development of a solution to eliminate the vulnerability from the IT system before harm is done.

Where possible and taking into account costs and existing knowledge, e-Contract.be BV will try to develop a solution with its subcontractors as soon as possible, depending on the severity of the risks for the users of the systems concerned.

At this stage, e-Contract.be BV and its subcontractors undertake to carry out, on the one hand, positive tests to check that the solution is working properly and, on the other hand, negative tests to ensure that the solution does not interfere with the proper functioning of the other existing features.

5.5 Possible publication

e-Contract.be BV will decide, in consultation with the participant, how the existence of the vulnerability may be published.

e-Contract.be BV also undertakes to collect users' comments on the application of the solution and to take the necessary corrective action to resolve any problems caused by the solution, including those relating to compatibility with other products or services.

6 Applicable law

Belgian law shall apply to any disputes relating to the application of this policy.

7 Duration and Updates

The rules of the policy apply from December, 1th 2021 until such time they are amended or annulled by e-Contract.be BV.

Any such amendments or annulments will be published on the e-Contract.be BV website and will automatically enter into force.

It is the responsibility of the participants to regularly review and stay informed about any changes, updates, or revisions to this policy. We may make modifications to this policy from time to time, and it is incumbent upon participants to ensure they are aware of the most current version. Participating after changes to this policy constitutes acceptance of the updated terms.