# RESPONSIBLE DISCLOSURE

| Author | Version | Date | Changes | Status |
|---|---|---|---|---|
| Erik Kempen | 1.0 | 05-05-2019 | Initial publication | Final |

## RESPONSIBLE DISCLOSURE STATEMENT

At eDomus we consider the security of our systems and the protection of your information a top priority. But no matter how much effort we put into system security, it is still possible that there are vulnerabilities in our website and related systems.

If you discover a vulnerability, we would like to know about it so we can take steps to address it as quickly as possible. We would like to ask you to help us better protect our clients and our systems.

**Code of conduct for responsible disclosure:**

- E-mail your findings to info@edomus.nl. Encrypt your findings with our PGP key to prevent the information from falling into the wrong hands. Do not take advantage of the vulnerability or problem you have discovered, for example by downloading more data than necessary to demonstrate the vulnerability or deleting or modifying other people's data;
- Do not reveal the problem to others until it has been resolved;
- Do not use attacks on physical security, social engineering, distributed denial of service, spam or applications of third parties, and
- Do provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible. Usually the IP address or URL of the affected system and a vulnerability description are sufficient, but for more complicated vulnerabilities more detailed information may be needed.
- We will respond to your notification within 5 business days;
- If you prefer to remain anonymous, we will not use or retain any personal data associated with the notification. You can also take steps yourself to ensure that the report remains anonymous by using an anonymous mail service on the Internet or via the TOR network.

*This code of conduct for notifying vulnerabilities in security at eDomus is subject to Dutch law.*