Security statement

IDfuse Holding and its underlying wholly owned legal entities (hereinafter: 'IDfuse'), are committed to protect its data and that of our clients from threats and/or threat actors like hackers, human errors, abuse, leakage, fire, theft and so forth. This is necessary to prevent damage to the interests of the parties involved – including IDfuse itself – and to be able to (continue to) provide effective, efficient, competitive and reliable services. Protection of information is set out in terms of Confidentiality, Integrity and Availability.

This statement is aimed at providing you with more information about our security practices. For more information about how we handle personal data, we refer you to our privacy statement [link].

Principles

The principles of information security within IDfuse reflect the organization values and thus create the basis for executing the information security management process:

- the board is accountable for information security related decisions and
- information security is a combined organizational effort, every IDfuse team member is responsible for contributing towards information security objectives in their role and related daily activities.

Objectives

IDfuse aims to provide trust and deliver impact to the consumer goods industry by, among others, adequate information security management. To support the achievement of these goals, IDfuse has established the following information security objectives:

- promote cybersafe behavior by continuously addressing information security awareness;
- composition of a governance structure by defining roles and responsibilities to create ownership and responsibility on information security across the organization.

How do we do this?

The board is accountable for information security, and therefor pay attention to the security and privacy responsibilities of its employees during onboarding. All employees within IDfuse are directly responsible for implementing and maintaining security for their respective business areas. It is the responsibility of all IDfuse team members to adhere to our security way of working. IDfuse uses the ISO 27001 norm for information security on several aspects to ensure adequate security in its systems.

Specifically, security at IDfuse is ensured through the following:

- IDfuse maintains access management, based on its RACI model.
- The board sets-up and maintains security policies and other controls based on ISO 27001 and the OWASP top 10, including access control, cryptographic control, version control, password policies and testing policies.
- In corporation with our partners, security is always part of the discussion. We aim to use security-by-design and privacy-by-design principles as much as possible in developing new functions or systems.
- IDfuse has controls in place to ensure adequate security for its digital environments by separating its environments, applying security monitoring and logging and using testing data in the development process.
- IDfuse uses processors with high standards for physical and network security. Therefore, IDfuse uses processors, whom are ISO 27001 certified.

Vulnerabilities

Although IDfuse takes security of our systems very seriously, there could be vulnerabilities which we don't know. If you have found a vulnerability, we kindly ask you to provide us with the information so we can mitigate the issue as quickly as possible. Please send us an e-mail at security@IDfuse.nl.

This security statement was drafted by Northwave Nederland B.V. commissioned by IDfuse.