Informatiebeveiliging bij Pipple

Extern informatiebeveiligingsbeleid

Ons commitment Pipple beschermt informatie van klanten, medewerkers, partners en andere belanghebbenden. Informatiebeveiliging is een integraal onderdeel van onze dienstverlening en bedrijfsvoering.

Beleid en reikwijdte

Pipple B.V. heeft een Information Security Management System (ISMS) ingericht voor het beheersen van informatiebeveiligingsrisico's. Het ISMS is gecertificeerd volgens ISO/IEC 27001:2022/Amd 1:2024 en wordt jaarlijks onafhankelijk geaudit. Het beleid geldt voor medewerkers, ingehuurde professionals en relevante leveranciers en partners binnen de scope van onze dienstverlening.

Certificaat: bekijk het actuele ISO 27001-certificaat

Onze uitgangspunten

- Vertrouwelijkheid: informatie is alleen toegankelijk voor geautoriseerde personen met een aantoonbare zakelijke noodzaak.
- Integriteit: informatie wordt beschermd tegen ongeautoriseerde of onbedoelde wijziging en blijft juist, volledig en betrouwbaar.
- Beschikbaarheid: informatie en systemen zijn beschikbaar voor geautoriseerde gebruikers wanneer dit voor de dienstverlening nodig is.

Hoe wij informatie beschermen

- Risicogebaseerde organisatorische en technische beveiligingsmaatregelen, passend bij de aard van de informatie en dienstverlening.
- Toegangsbeheer op basis van rollen en verantwoordelijkheden, persoonlijke accounts en waar passend multi-factor authenticatie.
- Bewustwording en periodieke training van medewerkers over informatiebeveiliging en privacy.
- Beveiliging van IT- en cloudomgevingen, inclusief back-up, herstel, monitoring, onderhoud en beheer van kwetsbaarheden.
- Vastgelegde processen voor incidentmelding, beoordeling, opvolging en continue verbetering.
- Afspraken over informatiebeveiliging en vertrouwelijkheid worden waar relevant contractueel vastgelegd met medewerkers, leveranciers en partners.

Naleving, verantwoordelijkheid en verbetering

Pipple werkt volgens toepasselijke wet- en regelgeving en contractuele verplichtingen op het gebied van informatiebeveiliging, privacy en gegevensbescherming, waaronder de AVG. De directie stelt middelen beschikbaar en bewaakt het belang van informatiebeveiliging. De dagelijkse coördinatie is belegd bij de aangewezen securityverantwoordelijke. Risico's, maatregelen, incidenten en doelstellingen worden periodiek beoordeeld, zodat het ISMS blijft aansluiten op veranderingen in technologie, wetgeving en dienstverlening.

Meer informatie: www.pipple.nl | incidentmanager@pipple.nl

Information Security at Pipple

External information security policy

Our commitment Pipple protects information belonging to clients, employees, partners and other stakeholders. Information security is an integral part of our services and business operations.

Policy and scope

Pipple B.V. operates an Information Security Management System (ISMS) to manage information security risks. The ISMS is certified to ISO/IEC 27001:2022/Amd 1:2024 and is independently audited every year. This policy applies to employees, contracted professionals and relevant suppliers and partners within the scope of our services.

Certificate: view the current ISO 27001 certificate

Our principles

- Confidentiality: information is accessible only to authorised persons with a demonstrable business need.
- Integrity: information is protected against unauthorised or unintended modification and remains accurate, complete and reliable.
- Availability: information and systems are available to authorised users when required for service delivery.

How we protect information

- Risk-based organisational and technical security measures appropriate to the nature of the information and services.
- Role- and responsibility-based access control, personal accounts and multi-factor authentication where appropriate.
- Awareness and periodic training for employees on information security and privacy.
- Protection of IT and cloud environments, including backup, recovery, monitoring, maintenance and vulnerability management.
- Documented processes for incident reporting, assessment, response and continual improvement.
- Information security and confidentiality requirements are contractually agreed with employees, suppliers and partners where relevant.

Compliance, responsibility and improvement

Pipple operates in accordance with applicable laws, regulations and contractual obligations relating to information security, privacy and data protection, including the GDPR. Management provides resources and promotes the importance of information security. Day-to-day coordination is assigned to the designated security responsible. Risks, controls, incidents and objectives are reviewed periodically, enabling the ISMS to remain aligned with changes in technology, legislation and service delivery.

More information: www.pipple.nl | incidentmanager@pipple.nl