Beveiligingsbeleid Invoyz B.V.

Versie AV2024-1.0

Dit beveiligingsbeleid beschrijft de maatregelen die worden genomen om de beveiliging van Invoyz te waarborgen. Het beleid is ontworpen om de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens en diensten te beschermen en te voldoen aan relevante wet- en regelgeving.

Statutaire naam: Invoyz B.V.
KVK: 92012582

Vestigingsadres: Louis Braillelaan 6
2719 EJ Zoetermeer
Nederland

Kantooradres: Louis Braillelaan 6
2719 EJ Zoetermeer
Nederland

Website: www.invoyz.com
E-mail: info@invoyz.com

Beveiligingsbeleid Invoyz B.V.

Versie AV2024-1.0

Artikel 1 Toegangsbeheer

1.1 **Identity and Access Management (IAM):** Invoyz gebruikt een centraal beheerd Identity and Access Management-systeem om gebruikersauthenticatie en autorisatie te beheren. Alle gebruikersaccounts zijn beschermd met Multi-Factor Authentication (MFA).

1.2 **Role-Based Access Control (RBAC):** Toegang tot functies en gegevens binnen Invoyz is gebaseerd op rolgebaseerde toegang, waardoor gebruikers alleen toegang krijgen tot de informatie die nodig is voor hun functie.

Artikel 2 Netwerkbeveiliging

2.1 **Firewalls en Inbraakdetectie**: Invoyz maakt gebruik van firewalls en inbraakdetectiesystemen om het netwerkverkeer te monitoren en te beschermen tegen ongeautoriseerde toegang.

2.2 **VPN en Versleutelde Communicatie**: Alle netwerkcommunicatie naar en van Invoyz is versleuteld via VPN's en gebruik van HTTPS/TLS om de veiligheid van gegevens in transit te waarborgen.

Artikel 3 Databeveiliging

3.1 **Versleuteling van Gegevens:** Gegevens die worden opgeslagen door Invoyz (data at rest) worden versleuteld met sterke encryptie-algoritmen. Gegevens die worden verzonden (data in transit) zijn ook versleuteld met behulp van SSL/TLS.

3.2 **Gegevensback-up:** Regelmatige back-ups van alle kritieke gegevens worden uitgevoerd en veilig opgeslagen. Back-ups worden getest om de beschikbaarheid en integriteit van de gegevens te waarborgen.

Artikel 4 Applicatiebeveiliging

4.1 **Beveiligde Ontwikkelingscyclus:** De ontwikkeling van Invoyz volgt strikte beveiligingsrichtlijnen met en het gebruik van geautomatiseerde tools om kwetsbaarheden te identificeren en te verhelpen.

4.2 **Input Validatie:** Om te voorkomen dat kwetsbaarheden zoals SQL-injecties en cross-site scripting (XSS) worden geëxploiteerd, wordt alle invoer gevalideerd en gesanitiseerd.

Artikel 5 Monitoring

5.1 Logboekregistratie en Bewaking: Invoyz bewaakt continu het systeemgebruik, logt belangrijke gebeurtenissen en heeft mechanismen om abnormale activiteiten te detecteren.

Artikel 6 Bedrijfscontinuïteit en Herstel

6.1 **Beschikbaarheid:** De infrastructuur van Invoyz is ontworpen om hoge beschikbaarheid te garanderen, met redundante systemen en failover-mechanismen