SECURITY POLICY LEVERANCIERS

VDL GROEP

VERSIE 1.0

KRACHT DOOR SAMENWERKING

INLEIDING

In de huidige digitale wereld is informatiebeveiliging van cruciaal belang voor het beschermen van bedrijfsgegevens en het waarborgen van de continuïteit van onze activiteiten. VDL streeft ernaar om informatiebeveiliging in al haar processen te borgen en verwacht hetzelfde van haar leveranciers. Deze security policy is opgesteld om duidelijke richtlijnen en verwachtingen te schetsen met betrekking tot de beveiligingsmaatregelen die haar leveranciers dienen te implementeren en na te leven.

Het doel van deze policy is om een gezamenlijke verantwoordelijkheid te creëren voor de bescherming van gevoelige informatie en om ervoor te zorgen dat alle betrokken partijen zich bewust zijn van hun rol in het handhaven van een veilige en betrouwbare samenwerking. VDL waardeert de samenwerking met onze leveranciers en gelooft dat door het naleven van deze richtlijnen, we samen een veilige en veerkrachtige werkomgeving kunnen creëren.

Vertrouwelijkheidsniveau	Publiek
Toepassingsgebied	VDL Groep
Versie	Versie 1.0
Datum printversie	04-12-2024
Auteur	Security Office
Afdeling	VDL ICT Security

INHOUD

2 POLICY ARTIKELEN

2.1 ALGEMENE VOORWAARDEN

De Leverancier zal alle toepasselijke wetten en voorschriften naleven, waaronder maar niet beperkt tot de AVG, DORA, NIS2 en de CRA.

2.1.1 Onderaanneming

De Leverancier zal ervoor zorgen dat eventuele onder-aannemers dezelfde (cyber)beveiligingsverplichtingen nakomen als de Leverancier onder deze Overeenkomst. De Leverancier blijft te allen tijde verantwoordelijk voor de naleving van deze verplichtingen door zijn onderaannemers.

2.1.2 (Cyber) Aansprakelijkheid

De Leverancier is aansprakelijk voor alle directe en indirecte schade die voortvloeit uit een inbreuk op de beveiligingsverplichtingen onder deze Overeenkomst. Deze aansprakelijkheid is niet beperkt door enige andere clausule in deze Overeenkomst.

2.1.3 Contractbeëindiging

Bij beëindiging van deze Overeenkomst zal de Leverancier alle IT-hardware, software, enz. die eigendom is van VDL Groep teruggeven en alle gegevens/activiteiten overdragen in een formaat dat compatibel is met open standaarden.

2.1.4 Locatie

De Leverancier zal de diensten uitvoeren en de gegevens verwerken op de locatie(s) zoals gespecificeerd in deze Overeenkomst.

2.1.5 Informatiebeveiliging

De Leverancier zal passende beveiligingsmaatregelen implementeren en onderhouden, waaronder beveiligings-testen, monitoring op afwijkingen, vulnerability management, en beveiligingsupdates/patching.

2.1.6 Retentierecht

Het eigendom van alle materialen en gegevens die door de Leverancier worden gebruikt of gecreëerd in het kader van deze Overeenkomst, gaat over op VDL Groep bij voltooiing van de diensten of bij beëindiging van deze Overeenkomst, tenzij anders overeengekomen.

2.1.7 Right to Audit

VDL Groep heeft het recht om audits uit te voeren om de naleving van de beveiligingsverplichtingen door de Leverancier te controleren. De Leverancier zal volledige medewerking verlenen aan dergelijke audits.

2.2 KWALITEIT VAN DE LEVERANCIER

2.2.1 Certificeringen

De Leverancier zal aantonen dat hij in het bezit is van relevante certificeringen (ISAE, SOC2 Type 2, ISO27001, TISAX, CYRA).

2.2.2 Processen en procedures

De leverancier zal passende procedures implementeren voor de volgende onderwerpen:

- security incident management,
- backup management,
- vulnerability management,
- patch management,
- monitoring,
- toegang voor personeel,
- achtergrondonderzoek (VOG).

2.2.3 Beveiligingsupdates/Patching

De Leverancier zal ervoor zorgen dat alle systemen en applicaties regelmatig worden bijgewerkt met de nieuwste beveiligingspatches om bekende beveiligingskwetsbaarheden te verhelpen.

2.2.4 Beveiligingsincidenten

De Leverancier zal alle beveiligingsincidenten onmiddellijk melden aan VDL Groep en zal alle redelijke maatregelen nemen om de gevolgen van dergelijke incidenten te beperken.

2.2.5 Beveiligingsbeoordelingen

De Leverancier zal regelmatig beveiligingsbeoordelingen uitvoeren en de resultaten van deze beoordelingen delen met VDL Groep.

2.2.6 Beveiligingsnormen

De Leverancier zal voldoen aan alle toepasselijke beveiligingsnormen en -richtlijnen, waaronder maar niet beperkt tot ISO 27001, NIST 800 series, en de Algemene Verordening Gegevensbescherming (AVG).

2.2.7 Toegangscontrole

De Leverancier zal passende toegangscontrolemaatregelen implementeren om ongeautoriseerde toegang tot de systemen en gegevens van VDL Groep te voorkomen.

2.2.8 Gegevensbescherming

De Leverancier zal alle persoonsgegevens die in het kader van deze Overeenkomst worden verwerkt, beschermen in overeenstemming met de toepasselijke wetgeving inzake gegevensbescherming.

2.2.9 Beveiligingstraining

De Leverancier zal ervoor zorgen dat al zijn medewerkers die toegang hebben tot de systemen en gegevens van VDL Groep, passende beveiligingstraining ontvangen.

2.3 KWALITEIT / BESCHIKBAARHEID VAN SOFTWARE / DIENST

2.3.1 Beschikbaarheid

De leverancier zal de beschikbaarheid waarborgen door maatregelen te nemen op de volgende onderwerpen:

- beschikbaarheid van systemen (RTO/RPO),
- continuïteit (escrow, continuïteitsregeling),
- IT continuïteit en DR procedures (recovery tijd),
- prestatie van leveranciers - monitoring/ SLR/ KPI.

2.3.2 Security testing

De Leverancier zal regelmatig beveiligingstesten uitvoeren, waaronder vulnerability scans en pentesten, om de beveiliging van de systemen en gegevens te waarborgen. De Leverancier zal alle bevindingen van deze testen rapporteren aan VDL Groep.

2.3.3 Vulnerability Management

De Leverancier zal een vulnerability management programma implementeren en onderhouden om bekende beveiligingskwetsbaarheden in de systemen en applicaties te identificeren en te verhelpen.

MEER WETEN?

Neem dan contact met ons op via onderstaande gegevens of kijk op **vdlgroep.com**

VDL Groep B.V.
Hoevenweg 1
5652 AW Eindhoven
+31 (0)40 292 50 00
info@vdlgroep.com

12-2024