Information security policy

Doel

OM DE KANS OP EEN SCHENDING VAN DE AUTHENTICITEIT, INTEGRITEIT, VERTROUWELIJKHEID EN BESCHIKBAARHEID VAN DE INFORMATIE, BRONNEN EN ICT-SYSTEMEN VAN AVEX TE MINIMALISEREN.

Informatiebeveiliging wordt gekarakteriseerd door het waarborgen van de vertrouwelijkheid (Bescherming van informatie tegen ongeautoriseerde toegang. Informatie is alleen toegankelijk voor degenen die daartoe bevoegd zijn.), integriteit (Zorgen voor de juistheid, volledigheid, tijdigheid en verifieerbaarheid van informatie en informatieverwerking.) en beschikbaarheid (Zorgen dat informatie en informatieverwerkingsmiddelen op het juiste moment en op de juiste plaats beschikbaar zijn voor de gebruikers.) van de informatie en de niet-weerlegbaarheid wanneer de informatie afkomstig is van een betrouwbare en geauthenticeerde bron. Bovendien zal informatiebeveiliging middelen bieden om vervalste informatie te weerleggen en het weerleggen van legitieme informatie onmogelijk te maken. Het informatiebeveiligingsbeleid is van toepassing op de gehele organisatie, inclusief alle processen, organisatorische eenheden, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid past binnen het algemene beleid van AVEX en relevante wetten en regelgeving.

Meer in het algemeen is het doel van dit beleid om schade te voorkomen die kan worden veroorzaakt aan het goed functioneren van de informatiesystemen die direct door AVEX of indirect door haar dienstverleners worden beheerd.

Informatiebeveiliging kan worden bereikt door het implementeren van passende beveiligingsmaatregelen die de risico's van de organisatie minimaliseren. Om dit doel te bereiken, moeten technische maatregelen worden geïmplementeerd, evenals beleidslijnen en procedures, en moet het personeel zich bewust zijn van informatiebeveiliging en deze beleidslijnen en procedures aanpassen.

Bij het bereiken van een goede basislijn van informatiebeveiliging houden we rekening met:

- Alle wettelijke bepalingen die relevant zijn voor informatiebeveiliging, zoals privacywetgeving of wetgeving inzake computercriminaliteit.
- Ons informatiebeveiligingsbeleid is het kader voor passende personele, organisatorische en technische maatregelen om informatie te beschermen en te waarborgen, zodat de organisatie voldoet aan de relevante wetten en regelgeving. De AVEX-aanpak is risicogebaseerd. Beveiligingsmaatregelen worden genomen op basis van een inventarisatie van de kwetsbaarheid en beschermingsvereisten van de informatie, de kwetsbaarheid van de werkprocessen.

Opeenvolgende risicobeoordelingen

De waarschijnlijkheid en impact van alle huidige risico's worden opnieuw geschat. Hebben de maatregelen erin geslaagd de waarschijnlijkheid en/of impact te verminderen? Zo niet, dan moet de risicodrager beslissen hoe het resterende risico moet worden behandeld (accepteren, mitigeren, vermijden of overdragen). Nieuwe risico's kunnen worden toegevoegd op basis van recente incidenten of actuele gebeurtenissen.

Acceptatie criteria

- Alle geïdentificeerde risico's moeten worden gemitigeerd tot niveau L;
- Risico's met niveau M score 3 of hoger, moeten binnen 12 maanden worden gemitigeerd;
- Risico's met niveau H score 6 of hoger, moeten binnen 3 maanden worden gemitigeerd;
- Het management moet op de hoogte worden gebracht van alle risico's met niveau M en H.

Houd er rekening mee dat uit een Management Review blijkt dat risico's kunnen worden geaccepteerd, zelfs als ze niveau M of H hebben.

De blootstelling wordt uitgedrukt als een factor van de waarschijnlijkheid en impact.

Waarschijnlijkheid / Impact	**High 3**	**Medium 2**	**Low 1**
High 3	H 9	H 6	M 3
Medium 2	H 6	M 4	L 2
Low 1	M 3	L 2	L 1

Waarschijnlijkheid

Waarschijnlijkheid	**Uitleg**	**Frequentie**
Low	• It is not likely to materialize • It has never happened to organizations similar to ours	Less than once per year
Medium	• It is likely to materialize • It has happened to organizations similar to ours	Once or twice per year
High	• It is very likely to materialize • It has happened to our organization before	Multiple times per year

Impact

Impact	Description	Financieel	Persoonlijke gezondheid	Reputatie	Rechtelijk
Low	• Sommige gegevens of informatie zijn niet nauwkeurig of beschikbaar • Kleine hoeveelheden niet-gevoelige persoonlijke gegevens gelekt • Kleine schade of gevolgen	Minder dan € 10.000	Eén persoon ervaart ongemak	Incidentele (lokale) media-aandacht	Een mogelijke claim
Medium	• De meeste gegevens of informatie zijn niet nauwkeurig of beschikbaar • Grote hoeveelheden niet-gevoelige persoonlijke gegevens gelekt • Aanzienlijke schade of gevolgen	Tussen € 10.000 en € 50.000	Meerdere personen ervaren ongemak, één persoon loopt letsel op	Incidentele landelijke media-aandacht of frequente lokale media-aandacht	Een rechtszaak, meerdere claims
High	• De meeste of alle gegevens of informatie zijn niet nauwkeurig of beschikbaar • Grote hoeveelheden gevoelige persoonlijke gegevens gelekt • Grote schade of gevolgen voor de continuïteit van de organisatie	Meer dan € 50.000	Meerdere personen lopen letsel op, fatale gevolgen	Frequente landelijke media-aandacht	Meerdere rechtszaken

Continu verbeterproces

Informatiebeveiliging is een continu verbeterproces. Binnen het kader van het informatiebeveiligingsbeleid, gebaseerd op het implementatieplan, wordt informatiebeveiliging continu verbeterd door middel van "plan, do, check en act". AVEX weet welke maatregelen zijn genomen en er is een planning van de maatregelen die nog niet zijn genomen. Dit alles is verankerd in een PDCA-cyclus.

Regels en verantwoordelijkheden voor het beveiligingsbeleid zijn vastgelegd en vastgesteld.

Alle medewerkers worden getraind in het herkennen van regels en verantwoordelijkheden, informatiebeveiligingsrisico's en het gebruik van beveiligingsprocedures.

Alle medewerkers, zowel vast als tijdelijk, zowel intern als extern, zijn verplicht om gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, wijziging, openbaarmaking, vernietiging, verlies of overdracht waar nodig en om vermoedelijke overtredingen te melden. Deze verplichting maakt deel uit van het arbeidscontract.

Scope

De reikwijdte van het informatiebeveiligingsbeleid omvat alle processen, onderliggende informatiesystemen, informatie en gegevens waarvoor AVEX wettelijk verantwoordelijk is, het gebruik daarvan door medewerkers, (keten)partners en klanten in de breedste zin van het woord, ongeacht locatie, tijd en gebruikte apparatuur.

Dit informatiebeleid stelt algemene beleidskaders vast. Specifieke (aanvullende) beveiligingseisen kunnen van toepassing zijn op (bepaalde) kerntaken op basis van wet- en regelgeving. Deze worden geïdentificeerd en beveiligd tijdens het classificatieproces.

Incidenten

Incidenten worden direct gemeld aan de Security Officer. Indien nodig wordt de NL/BE/LU/UK Data Protection Authority geïnformeerd. Passende maatregelen worden onmiddellijk genomen.

Externe partijen

Het informatiebeveiligingsbeleid, nationale normen en wet- en regelgeving zijn ook van toepassing op externe partijen (leveranciers, ketenpartners) waarmee de organisatie samenwerkt (of informatie uitwisselt). Ook voor externe partijen. Vereiste beveiligingsmaatregelen worden vastgelegd in contracten en/of verwerkersovereenkomsten. Deze omvatten onder andere dat beveiligingsincidenten onmiddellijk worden gemeld en dat de organisatie het recht heeft om overeenkomsten te laten controleren.

Voor de externe hosting van gegevens en/of diensten gelden de richtlijnen voor Cloud Computing in overeenstemming met het generieke informatiebeveiligingsbeleid. De organisatie is gebonden aan:

- Regels met betrekking tot grensoverschrijdend dataverkeer;
- Toezicht op naleving van regels door externe partij(en);
- De voorkeursleverancier van cloudservices is Microsoft Azure;
- Gegevens bij de Cloud Service Provider bevinden zich bij voorkeur in datacenters in de EU (West- en Noord-Europa);
- We zullen de versleuteldiensten van de leverancier gebruiken;
- Hoogste beveiligingseisen voor (speciale) categorieën persoonsgegevens;
- Rapportage aan de NL/BE/LU/UK Data Protection Authority bij overdracht van persoonsgegevens naar derde landen (buiten de EU);
- Meldingsplicht bij datalekken.

Beleidscyclus

Het informatiebeveiligingsbeleid is vastgesteld door het managementteam van AVEX. Het MT wordt geïnformeerd over de voortgang van de implementatie.

Plannings- en controlecyclus

AVEX stelt elk jaar een budget op, waarin de benodigde middelen voor informatiebeveiliging zijn opgenomen. De uitputting van het budget wordt gecontroleerd via de reguliere financiële rapporten.

Policy statements

- De verantwoordelijkheid voor alle inspanningen op het gebied van informatiebeveiliging is toegewezen aan de Security Officer.
- Beleids- en proceduredocumenten worden up-to-date gehouden en op verzoek beschikbaar gesteld aan alle relevante belanghebbenden.
- Training over bewustwording van informatiebeveiliging wordt aan alle medewerkers gegeven.
- Organisatorische en technische maatregelen worden genomen om informatie-assets te beschermen.
- Procedures worden ingevoerd om afwijkingen en incidenten te corrigeren en te voorkomen.
- We voldoen aan alle wetten en regelgeving in onze jurisdictie, in het VK, BE en NL.
- Om onszelf continu te verbeteren, herzien en definiëren we nieuwe doelstellingen.
- Om onze belanghebbenden zekerheid te bieden, streven we naar naleving van ISO 27001 en ISO 27017.
- We erkennen dat informatiebeveiliging in de Cloud een andere aanpak kan vragen dan legacy-systemen en -applicaties.
- Voor Cloud-setup volgen we deze richtlijnen:

- Versleuteling van gegevens tijdens overdracht moet end-to-end zijn.
- Versleuteling is belangrijk voor gegevens in rust.
- Kwetsbaarheidstests moeten rigoureus en doorlopend zijn.
- Er moet een gedefinieerd en gehandhaafd beleid voor gegevensverwijdering zijn wanneer het vertrouwelijke en gevoelige gegevens betreft.
- Er moeten proactieve lagen zijn met gebruikersniveau gegevensbeveiliging.
- Een virtueel privécloud en netwerk hebben.

Verantwoordelijkheden

- De Security Officer is verantwoordelijk voor het up-to-date houden van het beleid.
- Het management keurt het beleid goed na elke grote update.
- Het informatiebeveiligingsbeleid is van toepassing op alle belanghebbenden van onze organisatie.

Gerelateerde beleidslijnen

- Informatiebeveiligingsbeleid
- Toegangscontrolebeleid
- Back-upbeleid
- Cryptografiebeleid
- Ontwikkelingsrichtlijnen / beleidslijnen
- Informatieclassificatiebeleid
- Informatieopslagbeleid
- Logbeleid
- Wachtwoordbeleid
- Privacybeleid
- Leveranciersbeleid