Cyberbeveiligings-beleid (BAsic)

Sjabloon

# Autoriteit en herziening

## Documentcontrole en beoordeling

|  |  |
| --- | --- |
| **Documentcontrole** |  |
| Auteur |  |
| Eigenaar |  |
| Datum aangemaakt |  |
| Laatst herzien door |  |
| Laatste herzieningsdatum |  |

.

## Versiebeheer

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum van goedkeuring** | **Goedgekeurd door** | **Beschrijving van verandering** |
|  |  |  |  |

# Intro

**[Organisatie]** erkent de cruciale rol die informatie speelt in de hedendaagse bedrijfsdoelstellingen. In een moderne wereld moeten informatiesystemen in hoge mate met elkaar verbonden zijn en overal toegankelijk zijn. Hoewel dit grote kansen biedt, neemt het risico op vijandige aanvallen of verlies van gegevens snel toe.

Dit Cyberbeveiligingsbeleid bepaalt de minimumvereisten die van toepassing zijn op alle afdelingen van **[Organisatie]** zodat wij onze intellectuele eigendom, ons commercieel voordeel en onze mensen beschermen tegen de gevolgen van een slechte Informatiebeveiliging en eventuele cyberaanvallen.

Uiteraard worden ook de nodige aandacht gegeven aan het respecteren van wet-en regelgeving.

Waar van toepassing kunnen afdelingen aanvullende richtlijnen definiëren en aanvullende maatregelen nemen om het vereiste beveiligingsniveau te waarborgen.

# Beleidsprincipes

**We hanteren effectieve beleidsregels en procedures**

We zijn ons bewust van de risico's voor informatiebeveiliging. We maken samen beveiligingsbeleid en -procedures. We weten wie verantwoordelijk is en hoe we regels en procedures toepassen.

**We kennen onze omgeving en beheren risico's**

We hebben inzicht in welke informatiesystemen belangrijk zijn voor [Organisatie]. We kennen de risico's van deze systemen en houden deze op een acceptabel niveau. Een continue verbetercyclus zorgt ervoor dat onze beveiligingsniveaus zich blijven aanpassen aan wijzigingen in onze organisatie en omgeving.

**We bouwen veilige producten en/of diensten**

De producten en diensten van [Organisatie] worden gebouwd, getest en onderhouden met het oog op cyber-veiligheid en privacy.

**We onderhouden een robuuste infrastructuur**

De infrastructuur waarvan vitale systemen afhankelijk zijn, is ontworpen voor hoge beschikbaarheid.

**We handelen proactief**

We patchen regelmatig. We hebben inzicht in kwetsbaarheden in onze infrastructuur en blijven op de hoogte van nieuw ontdekte kwetsbaarheden. We leren van beveiligingsgebeurtenissen en -incidenten.

**We behandelen persoonsgegevens op een correcte manier.**

We verzamelen, gebruiken en bewaren persoonsgegevens conform de AVG ((EU) 2016/679). Dit betekent dat we de nodige technische en organisatorisch maatregelen voorzien.

# Toepassingsgebied

In het algemeen is dit Cyberbeveiligingsbeleid van toepassing op alle informatie en systemen van **[Organisatie],** samen met...

... de informatiesystemen die ze leveren,

... de mensen (interne en externe) die het verwerken,

... de apparaten die worden gebruikt om het te verwerken,

... de procedures waarvan het afhankelijk is,

… de locaties waar we werken

... de andere aspecten die een risico kunnen vormen.

Kritieke en vertrouwelijke informatie of systemen is informatie of systemen die de organisatie zal schaden wanneer de vertrouwelijkheid, integriteit of beschikbaarheid in gevaar is.

# Minimumvereisten

Onze omgeving wordt beheerd op een manier dat ze bijdraagt tot de cyberbeveiliging.

Dit omvat dat:

* De rollen en verantwoordelijkheden met betrekking tot cyberbeveiliging worden vastgelegd en gecommuniceerd naar zowel interne als externe betrokkenen.
* Er wordt een inventaris gemaakt en bijgehouden van alle binnen de organisatie gebruikte fysieke apparaten, systemen en software.
* Apparatuur die essentieel is voor kritieke systemen moet correct worden onderhouden om de blijvende beschikbaarheid en integriteit ervan te garanderen. Onderhoudscontracten of reserveonderdelen moeten worden overwogen.
* De door de organisatie goedgekeurde Antivirus, -spyware of andere -malware programma's moeten worden geïnstalleerd en bijgewerkt op de door de organisatie geïdentificeerde systemen en endpoints.
* Het bedrijfsnetwerk zal beveiligd worden volgens de vereisten vastgelegd in het netwerkbeveiligingsbeleid.
* Besturingssystemen voor zowel clients als servers en applicaties zullen voorzien worden van de nodige patches en beveiligingsupdates zoals beschreven in het Beleid rond het beheer van kwetsbaarheden en patches.
* Onze medewerkers en onderaannemers worden regelmatig bewustgemaakt van de cyberrisico's en -bedreigingen waarmee ze te maken kunnen krijgen en van hoe ze moeten reageren wanneer ze op een verdachte activiteit stuiten. **De 10 gouden regels voor cyberveiligheid** worden gecommuniceerd en elke werknemer of onderaannemer moet ermee instemmen deze regels na te leven.
* Er een gedegen Toegangsbeheer aanwezig is met de nodige aandacht voor;
  + Multifactor Authenticatie.
  + Minimale toegang. Gedetailleerd beleid wordt beschreven in het Toegangsbeleid.
  + Voldoende sterke wachtwoorden Gedetailleerd beleid wordt beschreven in het Wachtwoordenbeleid
  + Kritieke en vertrouwelijke systemen moeten op zijn minst succesvol aan- en afmelden loggen.
* Er een proces moet zijn om kritieke systemen te herstellen in het geval van een calamiteit. Er moet een proces zijn om kritieke documenten of records te herstellen als ze per ongeluk worden gewist. Gedetailleerd beleid wordt beschreven in het document Back-up en herstelbeleid.
* Er een responsplan aanwezig moet zijn in het kader van cyberincidenten.

Dit beleidsdocument maakt deel uit van een set van beleidsdocumenten die [Organisatie] ondersteunen bij het opstellen van een gedegen strategie rond cyberbeveiliging.