Informatiebeveiligingsbeleid

Deze template wordt u gratis aangeboden door het initiatief **Veilig Digitaal Ondernemen**. Het kan dienen als inspiratie voor uw eigen informatiebeveiligingsbeleid of gekopieerd worden  
 Vergeet dit blok niet te verwijderen en de nodige invulvelden aan te vullen.

# Bedrijfsgegevens

## Het bedrijf (hieronder genoemd als Het Bedrijf)

|  |  |
| --- | --- |
| **Bedrijfsnaam** |  |
| **Adres** |  |
| **Postcode + gemeente** |  |
| **Naam zaakvoerder** |  |

## De verantwoordelijke (hieronder genoemd als De Verantwoordelijke)

|  |  |
| --- | --- |
| **Naam verantwoordelijke** |  |
| **Telefoonnummer** |  |
| **E-mailadres** |  |

# Inleiding en doel

Dit informatiebeveiligingsbeleid beschrijft de maatregelen die Het Bedrijf neemt om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te waarborgen.

Het doel van dit beleid is om een kader te bieden voor het beschermen van bedrijfsinformatie tegen interne en externe bedreigingen en om te voldoen aan de NIS2-regelgeving.

# Toepassingsgebied

Dit beleid is van toepassing op alle medewerkers, contractanten en derden die toegang hebben tot de informatie en systemen van Het Bedrijf.

# Definities

**Informatiebeveiliging**: Het beschermen van informatie tegen een breed scala aan bedreigingen om bedrijfscontinuïteit te waarborgen, risico's te minimaliseren en investeringen en reputatie te beschermen.

**Incident**: Elk beveiligingsgerelateerd voorval dat mogelijk een negatieve impact heeft op de vertrouwelijkheid, integriteit of beschikbaarheid van informatie.

**Need-to-know principe**: Een beveiligingsconcept waarbij toegang tot informatie alleen wordt verleend aan individuen wier functie of rol deze toegang absoluut vereist om hun taken uit te voeren. Dit principe helpt om de blootstelling van gevoelige informatie te minimaliseren.

# Beleid

## Toegangsbeheer

* Toegang tot informatie wordt verleend op basis van het 'need-to-know' principe.
* Wachtwoorden moeten complex en regelmatig gewijzigd worden.
* Multifactor authenticatie (MFA) is verplicht voor toegang tot kritieke systemen.

## Gebruik van Bedrijfsmiddelen

* Bedrijfsmiddelen mogen alleen voor geautoriseerde doeleinden worden gebruikt.
* Het installeren van ongeautoriseerde software is verboden.
* Apparaten moeten up-to-date zijn met de laatste beveiligingspatches.

## Incidentbeheer

* Alle beveiligingsincidenten moeten onmiddellijk worden gerapporteerd aan De Verantwoordelijke.
* Er wordt een incident response team geformeerd om incidenten te onderzoeken en op te lossen.
* Regelmatige oefeningen worden uitgevoerd om de paraatheid te testen.

## Risicobeoordeling en -beheer

* Een jaarlijkse risicobeoordeling wordt uitgevoerd om bedreigingen en kwetsbaarheden te identificeren.
* Risico's worden beoordeeld en beheerd volgens de risicobeheerstrategie van Het Bedrijf.

## Compliance

* Het Bedrijf voldoet aan alle relevante wet- en regelgeving, inclusief de NIS2-regelgeving.
* Regelmatige audits worden uitgevoerd om naleving te controleren.

# Training en Bewustzijn

* Alle medewerkers ontvangen jaarlijkse training over informatiebeveiliging.
* Bewustmakingscampagnes worden regelmatig georganiseerd om medewerkers te informeren over de laatste dreigingen en best practices.

# Goedkeuring en Herziening

Dit beleid wordt jaarlijks herzien en goedgekeurd door het managementteam en De Verantwoordelijke van Het Bedrijf.

|  |  |
| --- | --- |
| **Aanmaakdatum** | \_\_\_\_ / \_\_\_\_ / \_\_\_\_\_\_\_\_ (dd / mm / yyyy) |
| **Datum laatste wijziging** | \_\_\_\_ / \_\_\_\_ / \_\_\_\_\_\_\_\_ (dd / mm / yyyy) |

|  |  |
| --- | --- |
| Handtekening zaakvoerder + datum | Handtekening De Verantwoordelijke + datum |