[bouwpas]

Directieverklaring

De directie van Bouwpas verklaart hierbij dat zij een managementsysteem voor informatiebeveiliging heeft geïntegreerd binnen de totale bedrijfsorganisatie. Bouwpas houdt zich bezig met: ***"Ontwerp, ontwikkeling, implementatie, beheer en support van SaaS met als doel het faciliteren van registratie, beoordeling en authenticatie van personeel".***

Dit managementsysteem voldoet tenminste aan de geldende wet- en regelgeving, klanteisen en wensen van de belangrijkste stakeholders, alsmede aan de continue verbetereisen die de ISO 27001 stelt aan het managementsysteem.

Het borgen van risico's

Bij het beschrijven van de organisatie en het inzichtelijk maken van het bedrijfsproces is beoordeeld of er voldoende beheersmaatregelen en middelen (opleiding / materieel / infrastructuur) beschikbaar zijn. Daar waar dat niet voldoende bleek, is het systeem aangescherpt. Tijdens de periodieke reviews wordt beoordeeld of het systeem nog adequaat is, en eventuele wijzigingen hierop aangegeven. In het beheer van de daaruit volgende maatregelen wordt voorzien door middel van de actielijst.

Klantwens

Binnen ons bedrijfsproces staat de wens van de klant centraal en daarmee de klanttevredenheid. Deze zorgt er namelijk voor dat onze continuïteit gewaarborgd blijft. De formulering van de klantwens is tot stand gekomen door de analyse van de klantcontacten. Deze wens is vertaald in de diensten die Bouwpas levert. In het managementsysteem staat beschreven hoe onze organisatie ervoor zorgt dat we hieraan blijven voldoen. Jaarlijks zullen de ervaringen en inzichten omtrent de klantwensen en andere relevante stakeholders worden geactualiseerd in een overleg voorafgaand aan de beoordeling van het managementsysteem.

Informatiebeveiligingsmanagementsysteem

Dit managementsysteem bevat de beschrijving van onze processen, waarbij de ISO 27001 als uitgangspunt is genomen. De directie is verantwoordelijk voor de correcte naleving van het systeem en dat het voldoet aan de wet- en regelgeving. De Security Officer is belast met het beheer van het managementsysteem en zorgt ervoor dat leidinggevenden de doelen van het managementsysteem hebben begrepen en in staat zijn de benodigde voorschriften uit te (laten) voeren. Aan alle medewerkers is opgedragen te voldoen aan wat in het protocol informatiebeveiliging is voorgeschreven. De directie zal volgens een vaste planning de implementatie en werking van het systeem (zoals procedures en werkvoorschriften) beoordelen.

Informatiebeveiligingsbeleid

Informatie is één van de belangrijkste middelen van deze organisatie. Het borgen van de toegankelijkheid en betrouwbaarheid ervan is een essentieel onderdeel van een verantwoorde bedrijfsvoering.

Informatiebeveiliging is de verzamelnaam voor de processen en maatregelen, die ingericht worden om de betrouwbaarheid van processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen al dan niet opzettelijk onheil. Het begrip "informatiebeveiliging" heeft betrekking op:

1. *Beschikbaarheid en continuïteit:*

Het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers.

2. *Exclusiviteit en vertrouwelijkheid:*

Het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

3. *Integriteit en betrouwbaarheid:*

Het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.

Informatiebeveiligingsdoelstellingen

Om het beleid m.b.t. informatiebeveiliging concreet te maken worden processen ingericht en continu verbeterd. De processen en de afspraken in het managementsysteem vormen tegelijkertijd de doelstellingen voor de organisatie m.b.t informatiebeveiliging. De prestaties van het systeem en daarmee ook de doelstellingen van de organisatie, worden beoordeeld en opgevolgd d.m.v. de jaarlijkse directiebeoordeling van het managementsysteem.

Toegankelijkheid op basis van need to know

Voor alle informatie en informatieverwerkende faciliteiten binnen de organisatie geldt dat het slechts beschikbaar wordt gesteld indien er een noodzaak is voor de betreffende persoon om de toegang te verkrijgen.

Noodzakelijke middelen ter beschikking stellen

Bij het beschrijven van de organisatie en het inzichtelijk maken van het bedrijfsproces is beoordeeld of er voldoende middelen (opleiding/materieel/infrastructuur) op het gebied van informatiebeveiliging beschikbaar zijn. Tijdens de periodieke review worden wijzigingen hierop aangegeven.

Correctieve, preventieve, en verbeterende maatregelen

Iedere medewerker binnen de organisatie heeft het recht én de taak om verbeterpunten en incidenten ten aanzien van informatiebeveiliging binnen de organisatie aan te geven middels digitale formulieren volgens de in het ISMS beschreven processen. Dit met als doel het continu verbeteren van de processen en zodoende nog beter aan de klantwensen voldoen. Een overzicht van de beheersmaatregelen ten behoeve van het managementsysteem voor informatiebeveiliging is opgenomen in de verklaring van toepasselijkheid.

Doelstellingen

Jaarlijks worden tijdens de beoordeling van het managementsysteem jaardoelen geformuleerd en geëvalueerd. Deze jaardoelen vormen samen met de stakeholders- en risicoanalyse en de verklaring van toepasselijkheid een integraal onderdeel van deze beleidsverklaring.

Haarlem, 11 juli 2023

Daan Verkaik

Directeur