Informatiebeveiliging Policy

Versie 1.0

24-Feb-2021

ONS BELEID

We streven in alles wat wij doen naar continue verbetering. Dit geldt ook voor informatiebeveiliging. Hiervoor hebben wij beleid geformuleerd dat als kader geldt voor onze doelstellingen en de risicobeheersing. Via de PDCA cyclus zullen wij dit beleid periodiek toetsen en verbeteren.

Strategisch beleid

De directie van Acterus kiest ervoor om het management van informatiebeveiliging in te richten volgens ISO 27001/ISO 27002 en in lijn met de relevante wet- en regelgeving.

Iedere medewerker kent het belang van informatiebeveiliging en past dit toe binnen het eigen werkgebied. De Gouden Regels zijn hierbij het uitgangspunt. Kennis en expertise zijn essentieel voor een bestendige Informatiebeveiliging en moeten geborgd worden. Alle medewerkers worden getraind in bewustwording voor informatiebeveiliging en het gebruik van procedures.

Informatiebeveiligingsbeleid

Binnen alle bedrijfsprocessen van Acterus vervult de informatievoorziening een cruciale rol. Acterus wil daarom op een verantwoorde manier met informatie omgaan, wat betekent dat de kwaliteit van informatievoorziening in control moet zijn. Een organisatie brede aanpak van informatiebeveiliging vervult hierin een sleutelrol. Wanneer informatiebeveiliging onvoldoende is ingericht, loopt de organisatie onnodige risico's. Deze kunnen leiden tot grote financiële schade, juridische gevolgen en imagoverlies.

Het vereiste kwaliteitsniveau van de informatievoorziening wordt bereikt door een passend stelsel van maatregelen, waarmee de beschikbaarheid, integriteit en vertrouwelijkheid van informatie wordt gewaarborgd. De pijlers van deze maatregelen zijn mensen, processen en techniek. Maatregelen worden in het informatiebeveiligingsproces genomen naar aanleiding van een risicoanalyse. De keuze van de passende maatregelen vindt plaats op basis van reële risico's die Acterus loopt.

Acterus streeft hierbij naar volledige compliance met betrekking tot de eisen zoals vervat in de stakeholdersanalyse), meest voornaam zijn hierbij:

- 0% dataverlies met betrekking tot digital assets van onze klanten
- Geen data breaches (datalekken), met name door falen van onze (logisch) toegangsbeveiliging of door toedoen van onze medewerkers.

Strategisch Beleid Onderwerpen

Ons beleid is op directie/strategisch niveau vastgesteld te worden.

Beleid voor mobiele apparatuur	Bedrijfs Devices worden uitgegeven (laptops), hiervoor geldt het beleid zoals omschreven in het Handboek IT (assetmanagement). Voor smartphones geldt een BYOD beleid waarbij momenteel geen technische maatregelen worden afgedwongen (lokale opslag van vertrouwelijke data is immers minimaal).
Beleid voor telewerken	Telewerken is toegestaan mits er gebruik wordt gemaakt van veilige verbindingen,
Beleid voor toegangsbeveiliging	Toegangsbeveiliging middels multi factor authenticatie (indien mogelijk) op basis van best effort en volgens het Need to know principe voor informatie die geclassificeerd is als vertrouwelijk en hoger.
Beleid inzake het gebruik van cryptografische beheersmaatregelen	Transport-, bericht- en data encryptie op basis voor systemen/data die zijn geclassificeerd als vertrouwelijk of hoger.
'Clear desk'- en 'clear screen'-beleid	Clear screen & clear desk beleid geldt voor vertrouwelijke en geheime informatie, voor zowel fysieke als IT werkplekken
Back-up van informatie	Back-ups worden op basis van classificatie rendundant uitgevoerd, bewaring (ook) buiten de fysieke locatie met een passende retentie en een bijbehorend testschema
Beperkingen voor het installeren van software	Installatie van (goedgekeurde) software mag door een admin worden uitgevoerd. Zie hiervoor ook ons changemanagement proces. Wij hanteren geen whitelist, goedkeuring verleend door Security Officer voor non admins.

Beleid en procedures voor informatietransport	Transport-, bericht- en/of dataencryptie indien systeem/data classificatie hiertoe noopt.
Beleid voor beveiligd ontwikkelen	Regels voor de ontwikkeling van software en systemen zijn opgedeeld in OTAP. Hierbij gebruiken wij beschermde ontwikkelomgevingen. Productie data (kopieën) mogen in test worden gebruikt.

4.4 Gouden regels

Binnen de Acterus gelden de volgende gouden beleidsregels:

1. Pas “Clear screen & clean desk” beleid toe.
2. Gebruik sterke wachtwoorden.
3. Beschik alleen over data die je echt nodig hebt (need to know principe) .
4. Scheid toegang tot data op basis van classificatie.
5. Bewaar/transporteer data alleen met goedgekeurde systemen en via goedgekeurde bedrijfsnetwerken (met passende beveiligingsmaatregelen).
6. Bewaar data altijd op een locatie die geback-upt wordt, m.a.w. data opslag altijd op Google Drive, niet op locale devices, tenzij essentieel voor werkzaamheden.
7. Hanteer alleen apparatuur die is toegestaan.
8. Maak geen verbinding met openbare netwerken, gebruik een veilige eigen hotspot.
9. Log altijd in op bedrijfsnetwerken met je eigen account, gebruik geen gedeelde accounts/wachtwoorden.
10. Pas de principes van secure development en secure architecture toe bij het beheer en ontwikkeling van software.
11. Pas de beveiligingsprincipes ook toe op leveranciers en ZZP’ers.
12. Meld verdachte situaties bij de Security Officer, door incidenten te blijven melden houden wij zicht op gevaarlijke/onwenselijke situaties.