BODEM – WATER – NATUUR

Titel:	ISO 27001 / 9001 Avallo Advies B.V.
Datum:	28 Februari 2023
Versie / status:	versie 3.01
Uitgever:	Avallo Advies B.V.
Naam:	Avallo Advies B.V.
Adres:	Binnenweg 8, 5757 PD Liessel

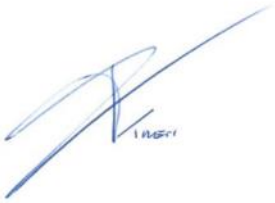
Voorwoord

Met de stap naar de ISO 27001 & 9001 certificering laat Avallo zien dat de juiste beheersmaatregelen genomen zijn om gegevens te beveiligen. Door de beschikbaarheid, integriteit en vertrouwelijkheid van deze gegevens te waarborgen. Voor u ligt het informatiebeveiligingsbeleid welke Avallo heeft opgesteld om aan de ISO 27001 & 9001 te voldoen.

De Directie van Avallo heeft dit beleidsdocument goedgekeurd en minimaal jaarlijks wordt het beleid gecontroleerd en mogelijk herzien . Bij significante wijzigingen in de organisatie wordt het beleid aangepast.

Jon Mensink (Directie)

Tom Mensink (Directie)

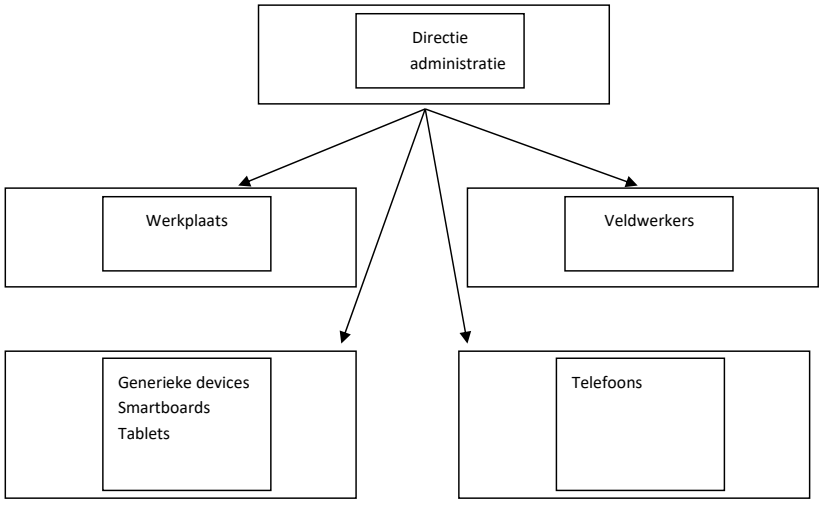


Bert van Bavel (Directie)

INHOUDSOPGAVE

1. BELEID VOOR MOBIELE APPARATUUR EN TELEWERKEN

Binnen Avallo worden meerdere mobiele devices(Apparatuur)gebruikt. De apparatuur kan conform onderstaande figuur verdeeld worden:



Figuur 1

Avallo is een relatief klein bedrijf en alleen een beperkte groep heeft toegang tot de administratie. De Directie en administratie van Avallo hebben voornamelijk werkzaamheden achter de computers. De veldwerkers leveren de data aan in specifieke projectmappen welke door de administratie en Directie verwerkt wordt.

1.1 REGISTRATIE VAN MOBIELE APPARATUUR

Zoals terug te zien is in Figuur 1 bestaat er binnen Avallo een hiërarchie van devices zoals de Directie-devices, Werkplaats-devices, Veldwerk-devices, Telefoons en randapparatuur (Smartboards tablets). De devices zijn benoemd om een overzicht te creëren. Hieronder een voorbeeld van de gebruikte codering:

Directie
D-0001-001-01
Werkplaats
W-0001-001-01
Veldwerker
V-0001-001-01

De letter staat voor de afdeling, het eerste getal staat voor het user nummer en het tweede getal als device type en als laatst het device user level. Specificaties betreffende het apparaat kunnen teruggevonden worden in de inventarisatie lijst.
Naast toegangsrechten en gebruik binnen het netwerk wordt de autorisatiematrix gebruikt tot welke systemen de werknemer/Useraccount toegang tot mag hebben. Er is een registratie voor het aanschaffen van nieuwe apparaten en onderhoud van deze systemen.

1.2 EISEN VAN SOFTWAREVERSIES EN MOBIELE APPARATUUR EN VOOR HET TOEPASSEN VAN PATCHES

Het beleid van Avallo is dat ten minst elke maand wordt gecontroleerd of er nieuwe patches zijn voor de geïnstalleerde software.

1.3 BEPERKING VAN VERBINDING MET INFORMATIEDIENSTEN

Om te zoeken op internet zijn de volgende tips opgesteld van voor het veilig gebruik van internet.

- Let op of de site authentiek is;
- Dat er een HTTPS verbinding is (zogenaamd slotje).

1.4 BESCHERMING TEGEN MALWARE

Voor de beveiliging tegen cyberthreat dienen de PC's en laptops over antivirus software te beschikken Avallo heeft gekozen voor ESET antivirus. Conform 1.2 worden de devices met Windows of andere besturing programma's met antivirus software gecontroleerd.

Met opmerkingen [G1]: Laten vervallen

1.5 OP AFSTAND ONBRUIKBAAR MAKEN EN OF WISSEN UITSLUITEN

Binnen Avallo wordt gebruikt gemaakt van 3 NASSEN (Network-attached Storage device) waarbij de eerste NAS als werkplek en opslag word beschouwd en de tweede NAS als back-up en afhaalpunt. De derde NAS is ingericht als IT-omgeving. Deze Nassen kunnen benaderd worden met het device wat aan de werknemer is toegewezen. Een gebruiker kan geblokkeerd worden wanneer dit nodig wordt geacht. Verder kan de gebruiker alleen bestanden lezen/aanpassen/wissen op de NAS in de mappen waar hij toegang tot heeft.

1.6 SCHEIDING VAN GEBRUIK APPARATEN EN INFORMATIIE PRIVE/ZAKELIJK

Het beleid is dat veldwerkers een device niet mee naar huis nemen. Indien dit onverhoopt toch voorkomt of noodzakelijk is dient de werknemer het apparaat met de nodige zorgvuldigheid af te schermen en bewaren. Avallo stelt de eis dat alleen de gebruiker toegang tot het device heeft. Voor een overzicht van de devices dient het uitleenschema benaderd te worden.

1.7 DRAAD/DRAADLOZEVERBINDINGEN

Binnen Avallo wordt gebruik gemaakt van de volgende verbindingen:

- Bedraad:

Dit is het bekabelde netwerk binnen Avallo, met dit netwerk kan verbinding worden gemaakt als een device hiervoor aangemeld / toegevoegd is binnen de inventarisatiemiddelen lijst. Toegang wordt geborgd met behulp van het MAC-adres van het device.

- Draadloos:

Dit is het wifi-netwerk(Avallo Werkplaats) van Avallo. Met dit netwerk kan enkel verbinding worden gemaakt mits met een wachtwoord en aanmelding. Toegang wordt geborgd met het MAC adres van het device.

- Simkaart:

Binnen Avallo zijn er ook devices die met een simkaart verbinding kunnen maken met het netwerk van Avallo doormiddel van een VPN. Hier vallen de volgende devices onder:

  - Laptops;
  - Tablets;
  - Smartphones;

- Thuis en Openbare netwerken:

Thuis en Openbare netwerken mogen gebruikt worden als deze goedgekeurd zijn door de ICT van Avallo. Avallo stelt de volgende eisen hier aan:

  - Als er gebruikt word gemaakt van wifi dient deze minimaal beveiligd te zijn met WPA2;
  - Is er een bedraad netwerk dan heeft dit de voorkeur.

Indien er de mogelijkheid is tot gebruik van Simkaart van het device dan heeft dit de voorkeur boven een thuis of openbaar netwerk.

1.8 DE BEVEILIGINGSEISEN DIE VOOR COMMUNICATIE GELDEN

Door de Directie worden specifieke opdrachten klaargezet in de veldwerkmap. Bij een regulier project zoals het plaatsen van peilbuizen heeft de projectleider afstemming met de klant over de werkzaamheden en kosten. Nadat de projectleider en klant tot overeenstemming zijn gekomen wordt de werkbeschrijving opgenomen in de map Veldwerk. Financiële gegevens worden opgeslagen in de map Projecten. Indien er specifieke eisen zijn ten aanzien van communicatie in het veld worden deze benoemd in de werkvoorbereiding. In de uitvoering kan er een afwijking optreden omdat de situatie buiten afwijkt van het aangenomen werk. Er is dan afstemming met de projectleider van Avallo. Deze besluit over de te nemen stappen. De afwijking met mogelijk financiële impact wordt daarna door de projectleider gearchiveerd. De veldwerker plaatst de (gewijzigde) veldwerkdata uit het veld in de daarvoor aangewezen digitale map.

1.9 DE BEDREIGING VAN ONBEVOEGDE TOEGANG TOT INFORMATIE OF MIDDELEN

Avallo heeft voor de verschillende gebruikers en functies van de systemen een autorisatiematrix opgesteld. Afhankelijk van het ingestelde niveau kan er gewerkt worden in de verschillende bestandsmappen. Voor de devices die aan een persoon of werknemer worden toegewezen wordt een bruikleenovereenkomst opgesteld. Voor apparatuur die enkel op kantoor staat is dit niet van toepassing.

1.10 GEBRUIK PRIVE APPARATUUR

Om dataveiligheid te borgen wordt binnen Avallo enkel met devices op de NAS gewerkt worden die opgenomen zijn in de Inventarisatie middelenlijst en in beheer zijn van Avallo.
Als er toegang dient te zijn tot de NAS omgeving van Avallo dient er een device van Avallo gebruikt te worden die aangemeld is op de inventarisatie middelen lijst, dit wordt tevens technisch afgedwongen binnen de firewall van de Cloud. Met privé apparatuur is er geen toegang tot de NAS.

1.11 SOFTWARE LICENTIE CONTRACTEN WAARDOOR DE ORGANISATIE AANSPRAKELIJK KAN WORDEN GESTELD

In de NAS-omgeving is de omgeving waar werknemers in werken ingericht. Er wordt gebruik gemaakt van een lokaal Laptop/PC computers waarop werknemers niet de mogelijkheid hebben om software te installeren, dit word afgedwongen door het besturingssysteem van de Laptop/PC. Om er zeker van te zijn dat er geen illegale software aanwezig is word dit periodiek gecontroleerd.

2. SCREENINGSBELEID

Avallo heeft een driekoppige Directie (Jon, Tom en Bert). Zij zijn gezamenlijk verantwoordelijk voor het implementeren en handhaven van het screeningsbeleid. Tot en met heden zijn de medewerkers aangedragen via het netwerk en is er geen actieve acquisitie nodig geweest. Met de implementatie van de VCA is de eerste stap gezet om de mensen die reeds werkzaamheden te verrichten ook bekend te maken met de protocollen en processen binnen Avallo. Verwacht wordt dat er in de nabije toekomst wel acquisitie nodig zou zijn om het team te versterken.

Het screeningsbeleid heeft betrekking op:

- Kandidaat medewerkers;
- Medewerkers die in dienst zijn (ook ZZP'ers die in dienst willen komen);
- Degenen die op bijvoorbeeld ZZP-basis werkzaamheden verrichten. Niet zijnde een arbeidsovereenkomst.

1e gesprek:
De kennismaking tussen de Directie en potentiële kandidaat. Hierbij wordt er op gelet wat de ambities en competenties zijn van de kandidaat. Avallo heeft erg specialistisch werk en er is geen vaste vooropleiding beschikbaar voor de werkzaamheden. Affiniteit met natuur, zelfstandig en oplossingsgericht en oog voor klantrelaties zijn essentieel in ons vakgebied. Bij Avallo kan vooralsnog onderscheid gemaakt worden tussen veldmedewerkers en staf. Voor staf zal een specifiek functieprofiel opgesteld moeten worden. Voor veldmedewerkers is het een allround functieprofiel.

De beste methode om te beoordelen of iemand binnen het bedrijfsprofiel past is dat iemand een werkdag meeloopt. Dit voorkomt verrassingen bij de potentiële kandidaat en Avallo.

2egesprek:
In het tweede gesprek wordt geëvalueerd of de meeloop-dag in lijn lag met de verwachtingen. Dit geldt zowel voor de kandidaat, als voor Avallo. Daarna wordt het contract (inclusief salaris) besproken. Op dit punt wordt ook het personeelshandboek overlegd, in het contract wordt namelijk getekend voor de regels/richtlijnen/verwachtingen die hierin vermeld staan.

De sollicitanten dienen bij een sollicitatie CV en relevante diploma's mee te nemen. Dit zodat Avallo kan verifiëren of de persoon daadwerkelijk is wie hij of zij, zegt te zijn.

Screening:

- Identificatie en controle van identiteit;
- Controle CV;
- Overleg van de relevante diploma's (inclusief rijbewijs);
- Indien mogelijk bellen van referenties;
- Afhankelijk van functie en verantwoordelijkheden VOG, indien iemand kantoorwerkzaamheden uitvoert dan wordt altijd een VOG geregeld.

- Wanneer iemand wordt aangenomen, wordt een personeelsdossier aangelegd. Hierbij wordt vastgelegd:
  - Getekend contract, hierin tekent men tevens voor akkoord personeelsbeleid zoals omschreven in het handboek.
  - Ingevulde inwerkchecklist (personeelsgegevens, huisregels, gedragscode en bedrijfsregelingen, Beleidsverklaring Avallo)
  - Indien aanwezig sollicitatiebrief;
  - Kopie identiteitsbewijs;
  - Kopie VCA diploma;

- Bruikleenovereenkomst mbt beschikbaar gestelde devices;
- Aanstellingsbrief nieuwe medewerker;
- Indien opgevraagd de VOG;
- Indien beschikbaar schriftelijke referenties;

Zoals eerder gesteld kan er onderscheid gemaakt worden tussen veldmedewerkers en kantoormedewerkers. Voor veldwerker is het mogelijk dat iemand wordt ingehuurd op ZZP-basis voor een kortere periode. Bijvoorbeeld omdat er tijdelijk extra inzet benodigd is in een project. In overleg met de Directie wordt vastgesteld in hoeverre deze persoon gescreend moet worden. Voor personeel dat op kantoor gaat werken dient er altijd een screening uitgevoerd te worden. Dit omdat deze medewerkers mogelijk met bedrijfsgevoelige informatie moeten werken. Daarnaast is er op kantoor ook eerder toegang tot bedrijfsgevoelige informatie. De verwachting is dat de kortstondige inzet van externen veelal in het veldwerk zal liggen. Voor het kantoorwerk heeft dit niet de voorkeur.

De Directie bestaande uit Jon, Tom en Bert is verantwoordelijk voor het structureel, in het personeelsdossier, (alleen) opslaan van relevante gegevens conform privacy wetgeving.

3. BELEID VOOR INFORMATIECLASSIFICATIE

Informatie dient geclassificeerd te worden om onderscheid te maken in beschikbaarheid, integriteit en vertrouwelijkheid. De verschillende soorten informatie binnen Avallo zijn geïnventariseerd en aan de hand daarvan geclassificeerd. In dit hoofdstuk wordt nader uiteengezet hoe om te gaan met informatie en/of hoe informatie gelabeld moet worden. Dit beleid is ingevoerd vanaf 2021, documenten voor 2021 zijn niet conform dit beleid gelabeld.

3.1 BENAMING DOCUMENTEN AVALLO

Avallo werkt op projectbasis. Er komt een aanvraag binnen en aan de hand van deze aanvraag wordt een specifieke offerte opgesteld voor het desbetreffende project. Veelal is de aanvraag middels de mail en kan er dan een aanvang worden gemaakt met het project. Elk project krijgt binnen Avallo een uniek projectnummer (jaartal 001). Op de offertes en facturen wordt het projectnummer vermeld. ~~Naast het projectnummer dient tevens de datum en de auteur te zijn vermeld. Voor de auteurs kunnen afkortingen worden gebruikt: zoals de intialen~~

Bijvoorbeeld: 202207681 Grondwatermeetnet Maashorst

Naast externe projecten zijn er ook interne projecten. Bijvoorbeeld het ontwikkelen van een alternatieve methode om peilbuizen te zetten. Ook hier wordt binnen Avallo een projectnummer voor aangemaakt. Projecten kunnen dus zowel extern als intern zijn. Avallo heeft de mappen ingericht op autorisatie en authenticatieniveau. Dit is terug te vinden in de autorisatie maplocaties en Bestandslabeling.

Een project start nagenoeg altijd met het opstellen van een offerte en mailwisseling. Avallo heeft veel kleinere projecten waarbij het niet efficiënt is om voor elk project een specifieke risicoanalyse te maken. Daarom heeft Avallo een standaard risicoanalyse opgesteld waaronder de reguliere projecten vallen. In de offerte aan opdrachtgever wordt in de bepalingen door Avallo aangegeven hoe de informatie wordt geclassificeerd (openbaar, intern of vertrouwelijk). Daarnaast wordt er verwezen naar ~~de Risicoanalyse die~~het informatiebeveiligingsbeleid welke eventueel op aanvraag beschikbaar is.

Elk project krijgt een uniek nummer en eigen map in de map projecten. Een beperkte groep medewerkers heeft toegang tot de map projecten. In elke map van de projecten wordt gewerkt in dezelfde sub-mappen:.

- Projectinformatie, hierin wordt zowel de ontvangen als zelf gegenereerde informatie opgeslagen. Een medewerker kan in deze map naar eigen inzicht eigen sub-mappen aanmaken. Dit is veelal afhankelijk van de grootte en complexiteit van een project;
- Gedeeld met klant, mails met offertes en/of losse offertes worden hierin opgeslagen. Dit zodat later eenvoudig teruggevonden kan worden welke informatie is gedeeld;
- Vertrouwelijke informatie, hierin wordt enkel informatie opgeslagen waarvan de klant of Avallo in overleg heeft bepaald dat deze vertrouwelijk is. Indien een klant aangeeft dat de informatie van het project geheel als vertrouwelijk moet worden aangemerkt zal er enkel in deze map gewerkt worden. Het kan ook specifieke informatie binnen het project zijn welke als vertrouwelijk wordt aangemerkt;
- Openbare informatie, dit is informatie welke na overleg met de klant extern kan worden gedeeld.

In de veldwerkmap wordt gewerkt met dezelfde projectnummers en omschrijving. In deze map staan standaard twee submappen:

- Aan te leveren, data welke is gecontroleerd door de Directie of veldwerker en gedeeld kan worden met de klant;
- Intern, data vanuit het project, een medewerker heeft de mogelijkheid om hier sub-mappen aan te maken.

Veelal is de aan te leveren informatie een selectie uit de interne data.

4. TOEGANGSBEVEILIGINGSBELEID

Toegangsbeveiliging heeft betrekking op zowel digitale als fysieke toegang. Medewerkers of derden welke toegang wensen of hebben verkregen dienen zich te conformeren aan het toegangsbeveiligingsbeleid van Avallo.

Niemand dient (te proberen) toegang te krijgen tot informatie waartoe hij niet bevoegd is of waar geen bedrijfsmatige noodzaak tot is. Indien iemand waarneemt dat hij toegang heeft tot informatie welke niet voor hem bestemd was dient deze persoon hier melding van te doen bij de Directie. Gebruikers (waaronder beheerders) die op meerdere niveaus toegang hebben tot systemen, dienen altijd de meest relevante toegang (waaronder in ieder geval de toegang met het minste privilege) te gebruiken.

Met opmerkingen [RJV2]: Heel goed!

4.1 DIGITALE TOEGANG

De digitale toegangsrechten van een werknemer staan in de autorisatiematrix. Indien geconstateerd wordt dat iemand toegang heeft zonder de juiste toegangsrechten dient dit gemeld te worden aan de Directie. Deze melding wordt genoteerd in de Incidentmeldingen lijst. Een werknemer met bepaalde functie kan in de autorisatiematrix zien tot welke applicaties en mappen hij toegang heeft. De Directie kan voor een functieprofiel applicaties toevoegen. Binnen een functieprofiel hebben alle werknemers dezelfde applicaties en wordt er geen onderscheid gemaakt.

Met opmerkingen [RJV3]: Dit stuk heb je ook al eerder beschreven. Het hoort hier natuurlijk, mogelijk op andere plekken weghalen? Of refereren naar dit stuk?

Systemen of applicaties (waar gevraagd wordt voor inlog gegevens) zijn enkel bereikbaar met een unieke gebruikersnaam en wachtwoord. In hoofdstuk 5; Wachtwoordbeleid, is dit verder uitgewerkt. Indien een werknemer alternatieve software wil gebruiken dient hij contact op te nemen met de Directie. Er wordt dan bepaald of de nieuwe software gebruikt kan worden en welk functieprofiel hiervoor toegang krijgt. De software wordt in de softwarelijst genoteerd en de autorisatiematrix wordt bijgewerkt. Avallo heeft gekozen voor een digitale omgeving in de NAS waar de informatie wordt opgeslagen. Een verzoek voor aanvullende toegangsrechten of nieuwe software dient altijd aangevraagd te worden bij de Directie. Dit verzoek wordt in overleg met IT-beheer verder onderzocht.

Met opmerkingen [RJV4]: Hoofdstuk 6 gaat naar H5. wachtwoordbeleid,

Met opmerkingen [RJV5]: Software installeren was toch niet mogelijk en niet toegestaan? Staat hierboven in het beleid voor mobiele apparatuur

4.2 FYSIEKE TOEGANG

Voor geprinte informatie is hetzelfde beleid van toepassing als voor digitale informatie. De Directie maakt mappen met geprinte informatie klaar voor het veldwerk. Deze geprinte projectinformatie is voor intern gebruik in het veld. Dit betreft veelal de tekeningen en werkvoorbereiding. Als er gevraagd wordt om specifieke geprinte informatie dient dit overlegd te worden met de Directie.

- Niemand bevindt zich buiten kantooruren (06:30-18:30) in het kantoor zonder toestemming te hebben gekregen van de Directie;
- Kantoor is buiten kantooruren afgesloten, fysieke toegang is dan niet mogelijk;
- Enkel de Directieleden en toegewezen personen zijn in het bezit van een sleutel. Jon zal ervoor zorgdragen dat het kantoor in overleg is geopend. Wanneer Jon afwezig is zal Tom of Bert het kantoor openen;
- Bij de ingang is een bel, bezoekers en leveranciers dienen zich aan te melden en worden ontvangen door een medewerker van Avallo. Deze medewerker blijft bij de bezoeker en draagt er zorg voor dat de bezoeker niet alleen in de kantoorruimte is;
- De kantoorruimte wordt afgesloten als er niemand aanwezig is. Bezoekers dienen zich te melden en worden geregistreerd en kunnen enkel met een medewerker van Avallo in de kantoorruimte zijn.

4.3 FYSIEKE BEVEILIGINGSZONES

Binnen het pand van Avallo kunnen de volgende beveiligingszones worden gedefinieerd:

- Hal, zone 1;
- Werkplaats Avallo, open gedurende kantooruren, wordt afgesloten buiten kantooruren, zone 4;
- Kantoorruimte Avallo, open gedurende kantooruren, wordt afgesloten buiten kantooruren, zone 2;
- Netwerkkast, afgeschermd en geplaatst op een moeilijk bereikbare locatie zone 6;
- Afgesloten kast waarin de devices liggen opgeslagen. Deze staat in de kantoorruimte. De sleutel wordt beheerd door Jon Mensink en/of Tom Mensink zone 2;
- Afgesloten kast openbare informatie wordt bewaard. Deze kast staat in de kantoorruimte zone 2;

De netwerkkast is tevens voorzien van bliksembeveiliging en UPS (Uninterupted Power Supply).

Bij het pand van Avallo melden bezoekers en leveranciers zich bij de hal. Bij de deur is een bel aanwezig welke in de kantoorruimte te horen is. De deur van de werkplaats is een garagedeur welke normaliter gesloten is en enkel wordt geopend indien nodig.

Het beleid is dat enkel de verantwoordelijke voor het ICT-onderhoud en de Directie in de netwerkkast (zone 6) mogen werken. Indien er gewerkt wordt in de nabijheid van de netwerkkast wordt dit geregistreerd.

5. WACHTWOORDBELEID

Binnen Avallo zijn er verschillende devices waar medewerkers met de juiste autorisatie kunnen inloggen. Persoonsgebonden wachtwoorden en aanvullende authenticatie middelen mogen niet worden gedeeld. Bij vermoeden van misbruik zal de Directie het betrokken account per direct blokkeren.

- NAS Avallo:

Mits een device is goedgekeurd door de ICT beheerder en aan de eisen voldoet kan er worden ingelogd in de NAS omgeving om aan projecten te kunnen werken.

- Applicaties derden:

De mogelijkheid bestaat dat een medewerker voor werkzaamheden in moet loggen in de omgeving van een derde. Hier worden de richtlijnen van Avallo aangehouden. Aan onderstaande specificaties moet een wachtwoord voldoen binnen de systemen van Avallo:

- De lengte van een wachtwoord(10):

De lengte van een wachtwoord moet minimaal 10 tekens bevatten.

- Hoofdletters, minimaal 1;
- Kleine letters, minimaal 1;
- Cijfers, minimaal 1;
- Speciale tekens, minimaal 1.

Met opmerkingen [RJV6]: 1,2,3?

Met opmerkingen [RJV7]: 1,2,3?

Het wachtwoord moet uniek in zijn soort blijven. Ook moet er op gelet worden dat een wachtwoord niet herleid kan worden naar een persoon, denk aan huisdiernaam of geboortenaam etc, dat maakt het mogelijk om wachtwoorden te 'raden'. Het beleid is dat een wachtwoord niet gelinkt is aan een wachtwoord wat in een privé omgeving gebruikt wordt.

Voorbeeld wachtwoord: De!Kat@Heeft#9$Levens% Een relatief makkelijk te onthouden wachtwoord maar vrij moeilijk te kraken. Avallo maakt gebruik van lastpass passwordmanager om wachtwoorden op te bergen.
Om de drie maanden moet een wachtwoord gewijzigd worden van:

- Fysieke apparaat wachtwoorden die genoteerd zijn in de Inventarisatie middelen lijst;
- NAS;
- Email;
- Eigen Portaal;
- Eigen Programma's(toekomstgericht).

Een wachtwoord mag maximaal 90 dagen gebruikt worden. Dit wordt technisch afgedwongen waar we het niet technisch afdwingen wordt een herinnering aangemaakt in de agenda. Wanneer een werknemer stopt bij Avallo worden de inlog gegevens ongeldig verklaard. Dit dient aan de Directie/ICT beheerder door gegeven te worden zodat dit account gedeactiveerd wordt.

5.1 ~~HET BELEID IS OM LASTPASS TE GEBRUIKEN VOOR HET OPSLAAN VAN WACHTWOORDEN.~~OMGAAN MET WACHTWOORDEN

Van werknemers wordt verwacht dat ze zorgvuldig met wachtwoorden omgaan. Indien wachtwoorden op computers of andere niet toegestane manieren worden opgeslagen dan wordt de werknemer hierop aangesproken en worden de wachtwoorden zo snel mogelijk veranderd. Mocht de situatie zijn dat de werknemer roekeloos met wachtwoordgegevens omgaat dan dient er een gesprek plaats te vinden en worden de wachtwoorden tijdelijk veranderd door de ICT beheerder/Directie.
Een werknemer mag het wachtwoordmanager-systeem alleen op bedrijf gerelateerde apparaten gebruiken. Het beleid is dat er enkel gebruik gemaakt wordt van Lastpass-passwordmanager.

6. CRYPTOGRAFIE

Avallo heeft de volgende beleidsregels opgesteld ten aanzien van cryptografie.

Avallo maakt gebruik van bitlocker op de apparaten waar bedrijf kritische data wordt opgeslagen. Sleutels van lokale devices worden lokaal opgeslagen en vernietigd door Directie en ICT-beheerder. Deze sleutels hebben een levenscyclus van 6 maanden.

Op de NAS (WerkomgevingAvallo / AvalloBAFH(Backup / uitlevermap~~)~~) wordt de data versleuteld door de NAS, dit wordt door middel van handmatige bewerking gedaan.

Met opmerkingen [RJV8]: Op welke manier? En wat zijn jullie eisen hieraan? Dit opnemen in het beleid

De eis van Avallo is de crypto grafische methode van AES256:

- DataAtRest (AES256)
- Encryptie op harde schijf niveau van devices waar bedrijf kritische data op staat (VM Omgeving, NAS);
- Encryptie binnen wachtwoord systeem;

Data in Transit
Minimale toepassing van SSL waarbij de voorkeur uit gaat naar TLS 1.2 Certificaten (Data transfer protocol);
HSTS-hypertextstrict transport Security (hiermee word gewaarborgd dat er enkel veilige site's bezocht worden. Veelal geïntegreerd binnen webbrowsers).

NAS van Avallo(Werkomgeving):

- Bij uitval of weghalen van de nas(AvalloOpslag) word de nas versleuteld met AES256 encryptie niveau;
- Encryptie binnen de Active Directory (locatie waar data verwerkt wordt binnen de NAS) van de NAS;
- Encryptie binnen wachtwoord systemen van applicaties (Last PASS);
- Encryptie op Database niveau (in transit).

Data kleiner dan 200mb wordt automatisch om het uur binnen de werkuren gecontroleerd met de virusscanner van de NAS. Bijzonderheden ten aanzien van encryptie of een bestand dient gemeld te worden aan de Directie en of ICT-beheer. Kritische crypto grafische sleutels worden beheerd door de ICT en Directie van Avallo.

Met opmerkingen [RJV9]: Ik zou hier een keuze in maken: Waar wil je alle incidenten gemeld krijgen?

Met opmerkingen [RJV10]: Hier schrijf je weer toekomst gerelateerd. Dit vind ik goed, maar neem dit dan wel over in implementatie actielijst!

Met opmerkingen [RJV11]: Dit zou natuurlijk goed zijn, nu nog de eisen hieraan stellen

7. CLEAR DESK EN CLEAR SCREEN BELEID

Avallo hanteert een cleardesk-, en clearscreen-beleid. Dit betekent dat papieren met (vertrouwelijke) informatie niet per ongeluk gedeeld kunnen worden met collega's, klanten of derden. Dit kan namelijk gezien worden als een informatiebeveiligingslek. Dit betekent niet dat een werkplek helemaal leeg moet zijn, maar voorkomt onbevoegde toegang van anderen. In de voorbereiding wordt er voor het veldwerk vaak een map voor in het veld gemaakt. Deze wordt per project klaargezet en overgedragen. Deze mappen staan in het kantoor per project gesorteerd. Is deze analoge data niet meer nodig dan wordt deze informatie vernietigd of digitaal verwerkt. Enkel de Directie heeft toegang tot de dossierkast. Binnen Avallo is eenieder bevoegd om een collega aan te spreken op het cleardesk-beleid.

7.1 ONBEHEERDE DEVICES

Na 10 minuten geen interactie met het device dient het device automatisch op slot te gaan. Dit is niet van toepassing voor RDP-omgeving. Het device moet versleuteld worden als men de werkplek verlaat (al is maar om naar het toilet te gaan). Veldwerkers dienen extra aandacht te hebben voor het beheren van het device in het veld. Denk daarbij voornamelijk aan het vergrendelen van de auto bij geen gebruik van het device. Dit beleid geldt voor alle devices.

7.2 ONBEVOEGD GEBRUIK VAN FOTO- EN KOPIEERAPPARATEN

Binnen Avallo is het niet toegestaan om zonder toestemming foto's te maken in het kantoor of werkplaats. In het veld mogen alleen foto's gemaakt worden van de opbouw van meetpunten die later verwerkt worden. Foto's moeten gemaakt worden met de devices die geregistreerd staan op de Inventarisatie middelen lijst. Verder dient er periodieke flushing plaats te vinden van de printer zodat er geen gevoelige data op de printer worden achtergelaten. Medewerkers mogen gebruik maken van de printer mits ze hier conform de Inventarisatielijst toestemming voor hebben. Vanzelfsprekend moeten geprinte documenten direct opgehaald wordt bij de printer. Papieren die blijven liggen bij de printer en opgemerkt worden door een medewerker dienen vernietigt te worden. Daarnaast moet de persoon die het vergeten is op te halen hierop worden aangesproken (incident).

8. BACK-UP BELEID

Voor back-ups is er een onderscheid tussen de lokale devices en de NAS. Beide omgevingen worden in dit hoofdstuk nader uiteengezet.

8.1 BACK-UPLOKALE OMGEVING

Van de lokale Laptop/PC die genoteerd zijn in de Inventarisatie middelen lijst worden systeem incrementele back-ups gemaakt voor het falen van de hardware. Op deze back-ups wordt geen encryptie toegepast. De back-ups van de systemen worden opgeslagen op de NAS. Binnen Avallo worden de back-ups bijgehouden op de NAS.
Bij kritieke verandering binnen het besturingssysteem, denk aan een patch, word er meteen een back-up gemaakt. Normaliter wordt de incrementele back-ups maandelijks uitgevoerd. Op de NAS kan nadere informatie over het verloop worden gevonden.

Met opmerkingen [G12]: Han, ik snap dit stukje niet helemaal

Met opmerkingen [A13R12]: Ik ook niet; heb wel de spelfouten eruit gehaald

Met opmerkingen [A14R12]:

Met opmerkingen [G15]: Clone of clones?

8.2 BACK-UP NAS

In de NAS van Avallo worden zowel snapshots als Externe back-up(naar een extern opslag apparaat) gemaakt:

Snapshot:

- Om de vijf minuten word er een snapshot gemaakt, he laatste snapshot van het uur wordt 12 uur behouden;
- Vervolgens word de laatste snapshot van de dag 3 dagen behouden;
- Waarbij de laatste snapshot van de week 1 week word behouden;
- Vervolgens de laatste snapshot van de maand 1 maand wordt behouden;
- De volgende mappen worden met snapshot overzien:
    - AvalloWiki;
    - Boekhouding
    - DeWatermeter;
    - Drone;
    - GIS;
    - ICTOnderhoudt;
    - Personeelsbeheer;
    - Planning;
    - Projecten;
    - Research And Development;
    - Veldwerk;
    - Werkplaats.

Externe Backup:
Binnen de NAS worden de ondergenoemde mappen om de dagelijks geback-upt naar een externe harde schijf hier is geen encryptie op toegepast:

- AvalloWiki;
- Boekhouding;
- chat;
- DeWatermeter;
- Drone;
- Foto’s;
- GIS;

- homes;
- ICTOnderhoudt;
- MailPlus;
- Personeelsbeheer;
- photo;
- Planning;
- Projecten;
- ResearchAndDevelopment;
- Veldwerk;
- Stagaire
- Werkplaats;
- Configuratie gegevens van ingestelde apps op AvalloOpslag;

Voor toepassing van de back-ups wordt verwezen naar het bedrijfscontinuïteitsplan en de procedure voor back-ups.

9. BELEID VOOR INFORMATIETRANSPORT

Informatietransport heeft betrekking op de volgende onderdelen:

- Digitaal en fysiek informatietransport;
- Informatietransport binnen de organisatie en met externen;
- Inkomend en uitgaande informatie.

Daarbij geldt als de algemene regel dat informatie alleen ontvangen of getransporteerd mag worden in overeenstemming met het opgestelde informatieclassificatie schema.

9.1 VERZENDEN INFORMATIE

Controleer de juistheid van de ontvanger (mailadres, telefoonnummer) communiceer niet wanneer het niet nodig is of wanneer onduidelijk is wie de informatie ontvangt (dit geld ook voor antwoordapparaten, voicemail of groep apps). Informatie of communicatie die onze organisatie kan schaden (o.a. laster, valse vertegenwoordiging, onbevoegd claimen van bevoegdheden) is niet toegestaan. Het heeft de voorkeur om informatie middels mail te versturen.

9.2 ONTVANGEN INFORMATIE

Informatie welke Avallo ontvangt dient alleen te worden opgeslagen op daarvoor bedoelde locaties, dit om te voorkomen dat gegevens onnodig vaak, of te lang, worden bewaard. Bijvoorbeeld een rapportage van een klant dient in de map van het bijbehorende project worden opgeslagen.

Informatie die wordt ontvangen op afroep (Downloads) dient gecontroleerd en geverifieerd te worden. Software die wordt gedownload mag alleen worden geïnstalleerd (Door Directie of IT) of toegepast indien deze is goedgekeurd door de Directie of op een lijst van goedgekeurde software staat. (zie softwarelijst)

Informatie welke bewaard moet worden dient conform het classificatieschema te worden bewaard.

9.3 DIGITAAL INFORMATIETRANSPORT

Het digitaal verzenden en ontvangen van informatie is mogelijk via diverse kanalen.

- E-mail;
- Synology chat
- Whatsapp;
- LinkedIN;
- Facebook;
- Wetransfer;
- Gespecialiseerde hardware(Peilbuizen, Hardware terminals).

Daarbij worden deze vormen van informatie transport beheerd door technische middelen zoals Firewalls. ICT-beheer is verantwoordelijk voor configuraties en applicaties, zoals toepasselijke routing, regels en controlemiddelen zoals Malware/Spam.

Op het hoogste niveau (Apps, gespecialiseerde hardware en API's) worden koppelingen alleen gerealiseerd door ontwikkelprojecten, waarbij de Directie betrokken is. Deze laatste kanalen zijn met name geschikt voor vertrouwelijke of bulk-overdracht van gegevens.
Informatie van het classificatieniveau "vertrouwelijk" mag alleen worden verzonden via door de Directie goedgekeurde systemen en met gebruik van de juiste templates.

Bedrijfsmatig gebruik van Social media zoals LinkedIN is alleen toegestaan na goedkeuring van de Directie. Informatie die als vertrouwelijk is geclassificeerd dient conform het kwalificatieniveau verwerkt of verstuurd te worden.

9.4 FYSIEK INFORMATIETRANSPORT

Onder fysiek informatie transport vallen de volgende onderwerpen:

- Handmatige overdracht van papieren documenten;
- Fysieke overdracht van digitale gegevensdragers (USB, harde schijven, enz.);
- Koeriersdiensten (Post NL, DHL, DPD, UPS);
- Post.

Bij informatietransport van vertrouwelijke informatie dient de ontvanger te tekenen voor ontvangst en wordt gebruik gemaakt van gespecialiseerde (veilig) vervoerders of mensen die in dienst zijn van Avallo. Informatie van categorie 'vertrouwelijk' dient aangetekend te worden verstuurd of worden overgedragen door een medewerker van Avallo. Ten voorkomen van verlies van informatie moet van unieke documenten een kopie gemaakt te worden ter (tijdelijke) archivering zolang de gegevens nog in transport zijn.

10. BELEID VOOR BEVEILIGD ONTWIKKELEN

Avallo is zowel bij de interne ontwikkeling van hardware en externe ontwikkeling van software betrokken.

10.1 INTERNE ONTWIKKELING

Binnen Avallo bestaat er een Hardware-matige/constructief ontwikkelomgeving. Dit betreft het ontwikkelen / configureren van meetpunten. Onder het ontwikkelen wordt het volgende verstaan:

Constructief Ontwikkeling
Het constructief ontwerp word schetsmatig en fysiek gebouwd in de werkplaats en later uitgewerkt op technische tekeningen.

Hardware-matige ontwikkeling/configuratie
Eveneens wordt het hardware-matige ontwerp gemaakt in de werkplaats. Mogelijk worden hier onderdelen gebruikt van derden. Dit geheel wordt later tot een totaal pakket geconfigureerd.

Om dit alles dataveilig te kunnen waarborgen heeft Avallo een R&D afdeling. Dit houdt in dat er een aparte account groep is binnen de NAS waar de Ontwikkeling word gedocumenteerd. Alleen Directie en aangewezen personeel hebben toegang tot deze omgeving. Het personeel dat hier toegang tot heeft, word aangewezen door een van de Directieleden en dient de gedragsverklaring van Avallo getekend te hebben.

10.2 EXTERNE SOFTWAREONTWIKKELING

Avallo kan betrokken raken bij externe soft en/of hardware ontwikkeling. Om een vertrouwensband met de desbetreffende leverancier te bewerkstelligen, dient er de mogelijkheid te zijn dat Avallo, de desbetreffende leverancier, kan auditen. Van de audit kun je het volgende verwachten:

- Capaciteit

Heeft de desbetreffende leverancier de juiste vaardigheden om het desbetreffende product te kunnen realiseren.

- Beleid betreft ontwikkeling

Om een beter inzicht te krijgen hoe een leverancier werkt kan er gevraagd worden naar het ontwikkelbeleid. Het onderwerp geheimhouding dient hier minimaal in uitgewerkt te zijn.

Dit alles wordt verwerkt worden in een zogenoemd audit document. Verdere afspraken worden vastgelegd in een leveranciers contract, hierbij wordt indien benodigd het audit document aan toegevoegd.

11. LEVERANCIERS

11.1 INFORMATIEBEVEILIGING LEVERANCIERS

Avallo maakt gebruik van verschillende leveranciers. Voor informatiebeveiliging kan er onderscheid worden gemaakt in diensten en producten. Bij de levering van producten zal er over het algemeen enkel mailwisseling en een factuur zijn.

Leveranciers van producten en diensten waarbij informatiebeveiligingsaspecten aan de orde komen worden jaarlijks beoordeeld aan de hand van de door Avallo opgestelde eisen. Hiervoor wordt het leveranciersbeoordelingsformulier gebruikt. Dit met betrekking tot de beschikbaarheid, integriteit en vertrouwelijkheid van onze informatie en informatiesystemen. Bij digitale diensten is het beleid dat specifieke contractuele afspraken vastgelegd worden in een contract. De basis voor deze contracten is het beleid van Avallo op het gebied van informatiebeveiliging. Indien er persoonsgegevens verwerkt worden dient er een verwerkingsovereenkomst getekend te worden. Vanuit Avallo dienen zowel leveranciers als verwerkingsovereenkomsten getekend te worden door de Directie.

Leveranciers krijgen enkel toegang tot onze informatie of systemen wanneer nodig. Indien er op het netwerk van Avallo gewerkt dient te worden dient dit gemeld te worden bij Directie. Deze toegang wordt geregistreerd.

11.2 KEUZE LEVERANCIER

Bij het inkopen van diensten en producten wordt er door Avallo een afweging gemaakt op basis van kwaliteit en prijs. Met de juiste keuze versterken we onze dienstverlening en daarnaast draagt het bij aan de rentabiliteit van Avallo. Het is dus belangrijk om bezig te zijn met de kosten.

In Januari 2023 is een analyse gemaakt op de 8 grootste kostenposten:

- Personeel → geen relatie met inkoop
- Management fee → geen relatie met inkoop
- Apparatuur Leiderdorp → afspraken liggen vast in een leveranciersovereenkomst. Prijs wordt voor een jaar vastgezet. Jaarlijks evalueren of de kwaliteit van het product in verhouding is tot de prijs en markt.
- Veldoffice → ontwikkeling Portaal continue evalueren. Bevindingen vastleggen in de leveranciersovereenkomst
- Auto's → investering in nieuwe auto's drukt zwaar op de liquide middelen
- Eijkelkamp → levering product
- Van Zeeland → levering PVC- schutkokers e.d.
- Diverse ZZPérs → jaarlijks evalueren of de diensten aansluiten

Afhankelijkheid van leveranciers

De prijs voor de hardware (apparatuur Leiderdorp) en het portaal (veldoffice) bepalen normaliter circa 50% van de kostprijs van een meetnet. Deze essentiële diensten/ producten zijn benodigd om een meetnet te exploiteren. Met uitslagen van tenders, overleggen met concurrerende aanbieders hebben we een vrij goed beeld waar deze producten in de markt staan. Met het portaal van Veldoffice is het mogelijk om voor andere apparatuur te kiezen. Uit verkennende gesprekken met Lizard blijkt dat het ook mogelijk is om voor het Portal over te schakelen.

Het beleid van Avallo is dat er een keuze wordt gemaakt op basis van prijs – kwaliteit voor het continueren van de dienstverlening en de levering van (vaste) apparatuur. Voor producten, nieuwe

apparatuur met een aankoopsom van meer dan 15.000 euro dienen minimaal 2 offertes opgevraagd te worden.

12. MELDEN INFORMATIEBEVEILIGINGS-INCIDENTEN

Avallo heeft een grote stap gezet op het gebied van informatiebeveiliging vanaf 2021. Essentieel is het blijven beschermen tegen ongewenste effecten. Daarom dienen alle medewerkers (en externen) relevante gebeurtenissen, incidenten en waargenomen kwetsbaarheden in onze systemen te melden bij de Directie of ICT-beheer. Dit kan ook een melding zijn van het gedrag. Eenieder binnen Avallo (ook de Directie) mag door eenieder worden aangesproken op het naleven van het opgestelde beleid:

Zie onderstaand enkele voorbeelden:

- Iemand heeft een vertrouwelijk document op de printer laten liggen;
- Iemand versleuteld zijn pc niet;
- Een bestand met persoonlijke gegevens staat in de verkeerde map of is simpelweg verdwenen;
- Deuren staan open;
- Kantoor is buiten openingstijden niet afgesloten;
- Iemand ontvangt een mail welke niet voor hem/ haar bestemd was;
- Wachtwoorden zijn onderling bekend (bijvoorbeeld op een papiertje bij de computer).

Meldingen worden altijd serieus genomen en vertrouwelijk in behandeling genomen. Iedereen binnen Avallo mag eenieder aanspreken op houding en gedrag ten aanzien van informatiebeveiliging.

12.1 CONTACT MET OVERHEIDSINSTANTIES

De meldplicht datalekken houdt in dat organisaties direct een melding moeten doen bij de Autoriteit Persoonsgegevens (AP) zodra er een ernstig datalek wordt geconstateerd. In overleg moet het datalek ook gemeld worden aan de betrokkenen en/of leveranciers. Dit zijn de mensen van wie de persoonsgegevens zijn gelekt. Een melding kan gedaan worden bij het meldloket datalekken
Meldplicht datalekken | Autoriteit Persoonsgegevens

Op de site van autoriteit persoonsgegevens kan het stappenplan worden gevonden wat gevolgd dient te worden bij een datalek. (zorg voor overzicht, beperk schade, wel/niet melden bij de AP, wel/niet melden aan de betrokken personen. Een datalek moet gemeld worden bij de AP tenzij het niet waarschijnlijk is dat het datalek een risico oplevert voor de rechten en vrijheden van de betrokken personen.

Het beleid van Avallo is dat, bij een melding, altijd iemand van de Directie betrokken is. Dit betekend dat indien de ICT-beheerder een lek constateert er direct contact wordt opgenomen met de Directie. Het is de verantwoordelijkheid van de Directie om indien nodig het datalek te melden bij de autoriteit persoonsgegevens.

13. ONTWIKKELINGEN INFORMATIEBEVEILIGING

Informatiebeveiliging is een actueel onderwerp waarin continue zaken aandacht blijven vragen. Voor Avallo is het van belang dat actuele items die Avallo kunnen schaden tijdig worden gesignaleerd. Denk hierbij een datalek van een organisatie die gebruik maakt van dezelfde software. Voor een leek zijn de ontwikkelingen moeilijk te volgen. Voor ICT-beheerders ligt er een professionele interesse in deze zaken. Om het juiste nieuws eruit te filteren wordt een beroep gedaan op de ICT-beheerder en zijn professionele vakkennis. De ICT-beheerder maakt voor het verkrijgen van zijn informatie gebruik van relevante websites en/of nieuwsbrieven. Het beleid is dat de ICT-beheerder en gedurende tijdens de jaarlijkse controle van het beleid afstemming hebben over de ontwikkeling in de informatiebeveiliging.

14. KWALITEITSBELEID

Een goed functionerend kwaliteitsbeleid is essentieel voor het verlenen van kwalitatief hoogwaardige en betrouwbare diensten aan onze klanten. Voor het bewaken en verhogen van de geleverde kwaliteit heeft Avallo beleid opgesteld.

Avallo heeft een grote diversiteit aan opdrachtgevers. Met deze opdrachtgevers hebben wij veelvuldig contact en stemmen wij de geleverde diensten nader af. In 2020 heeft Avallo de eerste stappen gezet om samen met deze klanten te evalueren of de geleverde diensten en producten in lijn lagen met de verwachting en of er verbeteringen mogelijk zijn. Deze evaluaties geven een extra klant-moment en bieden de mogelijkheid om de kwaliteit te verhogen. Daarnaast kan de opgehaalde informatie verwerkt worden in een zogenaamde tevredenheidsverklaring. Deze tevredenheidsverklaringen kunnen als referentie bij een nieuwe tender worden toegevoegd. In het managementoverleg van Avallo wordt besproken met welke klanten een evaluatie wordt uitgewerkt. Het doel is om jaarlijks met minimaal vijf klanten nader in gesprek te gaan over de geleverde diensten en dit samen vast te leggen (onderdeel beleidsverklaring 2020).
Naast het zogenaamde formele spoor dient er ook actief gewerkt te worden aan het wat minder formeel spoor. Dit is de verantwoordelijkheid van het gehele team van Avallo. Dit betekend regelmatig vragen of de geleverde dienst voldoet aan de verwachting. Bij nieuwe en bestaande relaties en voor alle projecten wordt met het gehele team de noodzaak van het leveren van kwaliteit overlegd.
Jaarlijks wordt er een stakeholder en verbeterplan uitgevoerd zodat er een volledig beeld is van de zaken die rondom de stakeholders spelen. In de SWOT matrix worden jaarlijks de interne en externe factoren in beeld gebracht (sterktes, zwaktes, kansen en bedreigingen).

14.1 MAATREGELEN TBV BORGEN EN VERHOGEN KWALITEIT

- Minimaal 5 evaluaties met als resultaat een volledige tevredenheidsverklaring;
- Jaarlijks uitvoeren stakeholder en contextanalyse;
- Jaarlijks uitvoeren risicoanalyse;
- Bedrijfsprocessen in beeld en actueel;
- Werkprotocollen.

Continue bespreekbaar maken kwaliteit in het gehele team en in de gehele organisatie uitstralen dat kwaliteit prioriteit nummer 1 is, dit wordt onderstreept in de beleidsverklaring van Avallo welke elke drie jaar wordt bijgesteld. Uit de eerder benoemde analyses komen acties om risico's en kansen op te pakken. In het managementteam worden deze acties besproken en wordt een planning opgesteld om opvolging te geven aan de actie. De maatregelen dragen bij aan het **continue verbeteren van Avallo**. De doelstellingen die geformuleerd worden dienen SMART (specifiek, meetbaar, acceptabel, realistisch en tijdgebonden) te zijn. Met de operationele planning en inrichting conform de ISO 9001 en 27001 wordt geborgd dat er voldaan wordt aan de van toepassing zijnde eisen.

14.2 INCIDENTEN TEN AANZIEN VAN DE GELEVERDE DIENST

Het is mogelijk dat er ondanks een gedegen voorbereiding een klant niet tevreden is. Het is belangrijk dat een klant zich dan gehoord voelt en een klacht/melding kan doen conform een uniforme procedure. Bij een standaard offerte is bij de bepalingen tevens de procedure ten aanzien van incidenten en klachten toegevoegd.

14.3 INTERNE BEDRIJFSPROCESSEN

Avallo maakt hiervoor onderscheidt in organisatieprocessen en operationele processen. De organisatieprocessen zijn ondersteunend voor het gehele bedrijf. De operationele processen hebben een directe relatie met de uitvoering, het zogenaamde veldwerk. Dit betreft werkprotocollen.

14.4 ORGANISATIEPROCESSEN

Voor de organisatie zijn de volgende relevante processen ten aanzien van het beheersen en verbeteren van de kwaliteit actueel:

- Primair bedrijfsproces, van aanvraag tot factuur;
- Managementproces, behouden technische kennis en voorlopen in innovatie;
- Ondersteunend bedrijfsproces, van facturen tot overzicht in bedrijfsresultaten;
- Ondersteunend bedrijfsproces, relatiebeheer;
- Ondersteunend bedrijfsproces, managen van veranderingen IT;
- Ondersteunend bedrijfsproces, managen van veranderingen;
- Ondersteunend bedrijfsproces, klachten professioneel verwerken;
- Ondersteunend bedrijfsproces, risico beoordeling en behandelprocedure.

In de sheet interactie tussen Processen Avallo is de samenhang tussen de verschillende processen in beeld gebracht.

Het beleid van Avallo is dat bovenstaande processen jaarlijks worden geëvalueerd.

14.5 OPERATIONELE PROCESSEN

Avallo voert een grote diversiteit aan werken uit. Het beleid van Avallo is dat activiteiten waar mogelijk geborgd moeten worden in een werkprotocol (digitaal)). Dit betekend dat het betreffende veldwerk conform een vooraf vastgestelde procedure wordt uitgevoerd. Dit verhoogd de kwaliteit en voorkomt faalkosten. Deze werkprotocollen worden indien mogelijk verwerkt in de veldwerkcomputers. Registratie van het veldwerk en op de juiste wijze uitvoeren van veldwerk zijn met behulp van het veldprotocol geborgd. De protocollen zijn gebaseerd op de van toepassing zijde NEN en kwaliteitseisen. Kleinere projecten kunnen met behulp van deze protocollen worden uitgevoerd. Voor grotere projecten kan aanvullend een uitvoeringsplan worden geschreven.

Met het opstellen van dit beleidsstuk en bijbehorende analyses en processen ten behoeve van de certificering voor de ISO 27001 en 9001 is een belangrijke stap gezet in het verhogen van de kwaliteit van de dienstverlening. Met deze normering heeft Avallo de handvatten in huis om conform een vast proces te werken aan het verhogen van de kwaliteit. De bedrijfsprocessen zijn uitgeschreven in het document Bedrijfsprocessen Avallo.

15. SANCTIEBELEID

Hoewel sanctiebeleid vervelend is voor zowel de werkgever als werknemer is het toch verstandig om dit onderwerp niet te mijden. Dit in de hoop dat het vastgelegde sanctiebeleid nooit toegepast hoeft te worden. Voor het niet naleven van het informatiebeveiligingsbeleid door medewerkers zijn disciplinaire maatregelen uitgezet.

- Allereerst een mondelinge waarschuwing door de Directie en eventueel een herhaling van deze waarschuwing;
- Een schriftelijke waarschuwing met de mededeling wat voor sancties er zullen volgen wanneer het voorval zicht herhaalt;
- Schorsing of non-actief;
- Ontslagaanvraag.

Bij een schriftelijke waarschuwing zal de werknemer moeten tekenen voor ontvangst. Alle disciplinaire maatregelen worden geregistreerd per werknemer.

16. WIJZIGING DIENSTVERBAND

De mogelijkheid bestaat dat iemand gedurende zijn werkzame carrière bij Avallo wijzigt van functie. In dat geval krijgt de medewerker andere rechten. Bij het wijzigen van het functieprofiel zal het nieuwe functieprofiel met de medewerker worden besproken. Indien als gevolg van de functiewijziging iemand andere toegangsrechten krijgt wordt dit nader toegelicht.

Indien een medewerker besluit zijn carrière elders voort te zetten zal er vanuit de Directie een exitgesprek worden gepland met de betreffende persoon. Voor dit gesprek heeft Avallo een standaard checklist welke doorlopen dient te worden.

Met opmerkingen [A16]: Hebben we deze checklist daadwerkelijk?

De Algemene Verordening Gegevensbescherming (AVG) schrijft geen concrete bewaartermijnen voor. Het uitgangspunt dat persoonsgegevens niet langer bewaard mogen worden dan noodzakelijk. Avallo heeft als beleid dat persoonsgegevens normaliter maximaal 6 maanden worden bewaard. Indien er bijvoorbeeld een juridische procedure loopt of andere zaken waarvoor het noodzakelijk is dat gegevens langer worden bewaard wordt dit overlegd met de werknemer. Bij de checklist van uitdiensttreding wordt de bewaartermijn vastgelegd.

17. BEGRIPPENLIJST

BEGRIP	DEFINITIE AANDUIDING
Administratie	De boekhouders/ personeelszaken
Autorisatiematrix	Een schema waarin vast is gelegd wie toegang krijgt tot welke persoonsgegevens.
Autorisatie niveaulijst	Lijst waarin staat tot welke devices/ software iemand toegang heeft
Avallo	Bedrijfsnaam
AVG	Algemene verordening gegevensbescherming De Europese privacywetgeving omtrent het beheer en de beveiliging van persoonsgegevens van Europese burgers
BIV-classificatie	Het indelen van (persoons)gegevens op basis van beschikbaarheid, integriteit en vertrouwelijkheid
NAS	De Cloud (Nederlands: wolk) staat voor een netwerk dat met alle computers die erop aangesloten zijn een soort “wolk van computers” vormt.
Data-integriteit	Data-integriteit heeft betrekking op de juistheid van de informatie. Is het niet verouderd of incorrect?
Device	Een Apparaat refererend naar PC, Tablet, Laptop etc.
Directie	De leidinggevenden binnen Avallo
Encryptie	Encryptie is het versleutelen van gegevens. Door de versleuteling kan een derde partij de gegevens niet inzien. Alleen de juiste zender en ontvanger beschikken over de sleutel
Grondwatermeetnet	Een systeem van verschillende peilbuizen om de grondwaterstand in het desbetreffende gebied te monitoren. Deze peilbuizen kunnen met loggers zijn uitgerust
Hacker	Een hacker is iemand die op zoek gaat naar zwakke plekken in computers, software of computernetwerken en vervolgens inbreekt.
ICT-coördinator – beheerder	Is betrokken bij de inrichting en beveiliging van het netwerk. Stemt met de Directie beveiligingsniveaus af en zorgt dat de beveiliging en software up to date is
ISO	Internationale organisatie voor standaardisatie. De ISO norm voor informatiebeveiliging is de ISO 27001 of 27002 of 9001
Leveranciers	Aanbieders van diensten of producten
Portaal de Watermeter	Een digitaal Portaal waar de gegevens van de sensoren beschikbaar worden gemaakt
SLA	Service Level Agreement – het onderhoudscontract tussen een organisatie en de leverancier van systemen, software of diensten