Beleid
Doelstellingen
Informatie Beveiliging

Inleiding

Beleid doelstellingen

Ten aanzien van kwaliteit is het beleid van Accensys gericht op het:

- Bewaken en optimaliseren van de klanttevredenheid en klantgerichtheid;
- Vergroten van de kennis en vaardigheden die bij werknemers in de organisatie aanwezig zijn;
- Blijven voldoen aan de eisen die worden gesteld vanuit wet- en regelgeving;
- Bieden van een raamwerk voor het bepalen van kwaliteitsdoelstellingen en continu verbeteren;
- Bewaken van de externe en interne kwaliteit en het continu verbeteren van de processen;
- Bijdragen aan duidelijkheid in de organisatie door middel van het vastleggen van verantwoordelijkheden, bevoegdheden, procedures en werkwijzen op kwaliteitsgebied;
- Bevorderen van eenduidigheid in werken, waardoor de kracht van onze werk methodiek tot zijn recht komt en bijdraagt aan ons succes;
- Leveren van diensten conform de gestelde eisen en focus op een gezonde balans tussen risico's en kansen.

De directie van Accensys houdt haar medewerkers van dit beleid en de daaruit volgende afspraken op de hoogte. Zij ziet toe op de uitvoering van dit beleid en stuurt, waar nodig, bij. De doelstellingen en Key Performance Indicatoren (KPI's) worden jaarlijks opgesteld en weergegeven in een jaarplan dat gecommuniceerd wordt naar alle medewerkers. De doelstellingen en KPI's worden proactief gemonitord, geëvalueerd en direct bijgestuurd waar nodig tijdens de diverse overleggen.

Eenmaal per jaar vindt een eind evaluatie plaats van de prestaties via de directiebeoordeling. Relevante delen van de verslaglegging zijn zowel intern als extern beschikbaar voor geïnteresseerden.
Accensys wil dat processen zoals deze verwoord zijn of waarnaar verwezen wordt in Accensys wiki omgevingen, als zodanig worden uitgevoerd door haar medewerkers. Alle medewerkers en ook derden die namens Accensys werkzaamheden uitvoeren ondersteunen dit beleid vanuit de eigen verantwoordelijkheid en betrokkenheid bij de kwaliteit van onze organisatie en onze dienstverlening.

De directie zorgt ervoor dat deze beleidsverklaring minimaal om de drie jaar wordt geëvalueerd en eventueel wordt herzien.
Informatie is essentieel geworden voor zowel het functioneren van onze bedrijfsvoering als voor de concurrentiepositie en de waarde toevoeging in onze producten en diensten. Denk bijvoorbeeld aan een business plan, personeelsinformatie of wachtwoorden. Enerzijds willen we deze informatie beschermen en veilig opslaan. Anderzijds moet er ook met deze

informatie kunnen worden gewerkt.
De directie van Accensys heeft er derhalve voor gekozen dat het managementsysteem van Accensys moet voldoen aan de vereisten zoals vastgelegd in de norm ISO/IEC 27001. Deze norm beschrijft de manier waarop Accensys om moet gaan met het onderwerp informatiebeveiliging. De voorlopers (BIS, NEN) van deze norm hadden een voorschrijvend karakter ('doe dit, doe dat'), maar ISO/IEC 27001 sluit aan bij de opzet die praktisch alle managementsystemen volgen: *Continue verbetering van processen (PDCA-Plan, Do, Check, Act)*.
Informatie dient te worden gezien als een aspect of kenmerk van een proces.

Voorbeelden:

- Informatie van de klant die nodig is om een product te kunnen installeren en opleveren, gaat met de orderstroom mee;
- Informatie over de klant zit in een klantdossier en in mailingen om informatie te delen;
- Een e-mail waarin de klant de order bevestigt, is onderdeel van de overeenkomst;
- Functioneringsgesprekken leiden tot verslagen en personeelsdossiers.

Er is ook informatie waar we niet direct mee werken, maar die wel essentieel is. Denk aan:

- De oprichtingsakte van een Accensys vennootschap;
- De back up van een server;
- Afspraken in een arbeidscontract of algemene leveringsvoorwaarden.

Vervolgens houden we nog rekening te met de informatiedragers c.q. de media. Een back up staat op een harde schijf, tape of onze storage in een datacenter. Informatie staat in diverse mail boxen, zoals verzonden items, verwijderde items en ontvangen items van verschillende collega's. ISO/IEC 27001 vraagt ons om goed na te blijven denken over de media, opslag en gebruik.
Alles bij elkaar opgeteld, is het de vraag voor Accensys op welke wijze met processen alsook hun informatie wordt omgegaan. De keuzes in de procesbeheersing hangen grotendeels af van de eisen van klanten, andere stakeholders en richtlijnen in de wet. Daarnaast heeft Accensys natuurlijk ook een eigen visie. Accensys zorgt dat de mate van procesbeheersing aansluit bij de missie, visie en doelstellingen van Accensys en zorgt dat deze geïntegreerd zijn in de maatregelen en procedures die zijn vastgelegd in het bestaande managementsysteem. Daarmee is het *Accensys Information Security Management System (Accensys ISMS)* integraal onderdeel van ons operationele managementsysteem.

Beleid doelstellingen informatiebeveiliging

Ten aanzien van informatiebeveiliging is het beleid gericht op:

- De juiste omgang met vertrouwelijke gegevens;
- Informatie van de eigen organisatie eveneens veilig is;
- Informatie die alleen beschikbaar is voor functionarissen die volgens de processen, functie omschrijvingen en bedrijfsreglement toegang toe hebben;
- Informatie van Accensys zelf, van klanten en medewerkers als ook informatie over producten en diensten alleen beschikbaar voor medewerkers van de eigen organisatie.

Hieruit volgen specifieke maatregelen, die zijn afgeleid van en die passen bij de eisen van stakeholders, de wetgeving, de norm ISO/IEC 27001 en natuurlijk de vereisten van Accensys zelf, gekoppeld aan de missie en visie.
Deze maatregelen komen voort uit het mechanisme om de informatiebeveiliging continue op een hoger niveau te brengen: procesmanagement, de continue verbetering van processen. Dit gebeurt enerzijds via het continue meten en analyseren van processen en anderzijds uit het maken van periodieke risico analyses.
De doelen – de proces prestatie niveaus – die Accensys ten aanzien van informatiebeveiliging wilt bereiken, worden middels de beleidscyclus bepaald en via de jaarplanning gerealiseerd. De doelen worden vertaald naar doelen voor afdelingen en individuele medewerkers. Ze worden vervolgens gemeten, waarna wordt bijgestuurd en gecommuniceerd. De informatiebeveiliging wordt verbeterd en risico's gereduceerd.
Uiteraard is de directie van Accensys eindverantwoordelijk voor een juiste invoering, uitvoering en het onderhoud aan het informatie beveiligingssysteem als onderdeel van het algemene managementsysteem. De praktische invulling hiervan is het hiervoor genoemde *Accensys Information Security Management System*. De directie tezamen met het management team voert periodiek risicoanalyses uit, onderzoekt kansen, meet de resultaten van processen en stelt verbeteringen voor.
De medewerkers zijn binnen hun functie en werkgebied verantwoordelijk voor de juiste uitvoering van procedures. Naast dat zij kennis moeten hebben van het managementsysteem en het *Accensys Information Security Management System* als onderdeel daarvan, ontvangen zij diverse proces documenten, het ICT Beleid, het ICT Beveiligingsbeleid en de *ICT gedragscode* waarvan zij verklaren hiernaar te handelen.

Uitwerking beleid

In onderstaande paragrafen wordt een korte uitwerking van het beleid toegelicht op de volgende onderdelen. Het beleid ten opzichte van;

- Leveranciers
- Mobiele apparatuur
- Software updates en patches
- Telewerken
- Softwareontwikkeling
- Toegangsbeveiliging
- Cryptografische maatregelen
- Backup van data
- Installeren software op operationele systemen
- Data-transport
- Clear desk/screen

Leveranciers

Bij het aangaan van een samenwerking met een externe partij word er gekeken naar de manier waarop de leverancier bijdraagt aan de korte en lange termijn doelstellingen van onze organisatie. Wanneer noodzakelijk wordt er een schriftelijke overeenkomst opgesteld waarin de voorwaarden van de samenwerking worden vastgelegd.

Leveranciers worden geclassificeerd naar het belang van de verwerking van informatie van Accensys en/of haar relaties. Hoe groter dit belang hoe hoger de eisen aan informatiebeveiliging worden gesteld. Dit varieert van een verwerkersovereenkomst (AVG) tot aan de eis van ISO27001 certificering.

Mobiele apparatuur

Het beleid voor het gebruik van mobiele apparatuur (Laptops, GSM, USB-sticks, externe disks) is vastgelegd in diverse documenten. Het belangrijkste document is de gedragscode. Alle medewerkers tekenen bij in dienst treden bij Accensys kennis te hebben genomen van de gedragsregels.

Software-updates / patches

Accensys draait veilige en betrouwbare software met een goede ondersteuning door de leverancier. Voor het beleid rond IB van de software gebruik zijn de volgende regels van kracht:

- Kritieke en security patches moeten zo snel mogelijk geïnstalleerd worden. Hiermee kunnen we ernstige kwetsbaarheden zo veel mogelijk voorkomen.
- Software updates worden eerst getest en dan pas uitgevoerd.
  We willen uiteraard voorkomen dat een update nieuwe fouten introduceert. Voor patches zal een beperkte test afdoende zijn. Voor service en major updates is een uitgebreide test en een implementatieplan vereist
- We lopen maximaal 1 major versie of 2 LTS versies achter bij de nieuwste beschikbare versie.

Telewerken

Accensys staat haar medewerkers toe, mits gehouden aan de regels "gebruik mobiele apparatuur" en "bring your own devive", thuis of vanaf een ander adres in te loggen op de IT-infrastructuur van Accensys. Men uitsluitend in met behulp van een VPN beveiligde verbinding.

Softwareontwikkeling

Binnen de organisatie wordt software ontwikkeld. Het betreft hier zowel "standaard software" die als product in de markt gezet worden als maatwerk ontwikkeling voor eigen gebruik of in opdracht van klanten. Beleid is dat bij het specificeren van de functionaliteit van de software aandacht wordt besteed aan de informatiebeveiligingsaspecten van het eindproduct. Accensys hecht grote waarde aan het gebruik van bekende systemen en technieken (bijvoorbeeld SQL server en c#).

De werkzaamheden zijn gevangen in een vastgesteld proces waarin de veiligheid gewaarborgd wordt intern testen alvorens de software wordt aangeboden ter acceptatie aan de klant (OTAP).

Toegangsbeveiliging

Het uitgangspunt voor het beleid van toegangsbeveiliging is "least privilige". Op basis van functiescheiding zijn er aan medewerkers personal credentials uitgedeeld welke centraal worden beheerd. Toegang tot data binnen de infrastructuur van Accensys is slechts toegankelijk via multi factor authenticatie.

Er wordt gebruik gemaakt van externe partijen om lacunes in de technische maatregelen te identificeren. Hiertoe laat Accensys periodiek een pentest op de netwerk infrastructuur uitvoeren.

Cryptografische maatregelen

Voor de beveiliging van de gegevens op devices is het beleid "encryptie". Voor netwerkcommunicatie worden standaard certificaten mee geleverd, afhankelijk van de mate van beveiliging die vereist is.

Back-up van data

Tegen verlies of verminking van data biedt Accensys back-up diensten. Beleid is dat voor alle data een dagelijkse back-up draait in het data center van Accensys op disk, een shadow copy wordt weggeschreven op disk buiten het data center van Accensys én een back-up op tape wordt uitgevoerd, welke buiten het data center wordt bewaard. Het gebruik van tapes gebeurt met verschillende frequenties, namelijk dagelijks, wekelijks, maandelijks en jaarlijks. Deze tapes hebben een verschillende bewaartermijn. Voor relaties is de retentie van de back-up zelf te bepalen.

Er worden periodiek restores uitgevoerd om de data-integriteit te bewaken van de back-ups.

Installeren software op operationele systemen

Accensys heeft een groot belang bij betrouwbare en veilige systemen. Een van de manieren om dit te waarborgen is het beperken van de software die op deze systemen geïnstalleerd mag worden. Op werkstations is er een lijst met door Accensys toegestane software beschikbaar. Voor software op netwerkservers wordt software getest op niet-productie servers alvorens de software in productie wordt genomen.

Datatransport

Uitwisselen van klant data via een datalijn wordt uitsluitend versleuteld tussen bron en ontvanger uitgevoerd. Voor transport van data middels gegevensdragers wordt gezorgd voor een juiste registratie en beveiliging van de gebruikte gegevensdragers. Informatie uitwisselen via open communicatiekanalen is alleen toegestaan met versleuteling van data.

Clean desk en clear screen

Beleid is dat er geen documenten met gevoelige informatie of gegevensdragers onbeheerd achter worden gelaten op de werkplek. Bij het verlaten van de werkplek moet het beeldscherm worden vergrendeld.