Johan

Beleid Informatiebeveiliging Johan BV

Opsteller: G. Westerlaken
Versienummer: 1.4.1
Datum 1e versie: 01-11-2019
Laatste revisie: 30-03-2020
Status: definitief, goedgekeurd door directie.
Documentnaam: Beleid Informatiebeveiliging Johan BV.docx

Classificatie: openbaar.

History:

Versie 1.1
Toegevoegd t.o.v. conceptversie 1.0: paragraaf 3.1.1 en 3.1.2
Aangepast t.o.v. conceptversie 1.0: hoofdstuk 5, doelstellingen IB
Versie 1.2 Professional rol benoemd in paragraaf 3.1.1
Versie 1.3 Doelstellingen uitgebreid
Versie 1.4 Doelstellingen aangepast, kleine tekstuele aanpassingen

Link met andere relevante documenten

Openbaar:

- ISO 27001 Verklaring van toepasselijkheid
- ISO 27001 Certificaat
- Privacyverklaring JOHAN BV
- JOHAN Portaal - Eigenaarschap van data, borging privacy en de AVG
- Privacybeleid Johan BV
- Ethische code Johan BV

Intern vertrouwelijk, op verzoek ter inzage:

- Technische beschrijving en security aspecten Johan Portaal
- Beveiligingsnormen voor systeemontwikkeling
- Risico assessment en behandel methodiek Johan BV
- Continuïteitsplan Johan BV

Inhoud

1 Inleiding 3

2 Verantwoordelijkheid, doelstelling en doelgroep 3

3 Toepassingsgebied 3

3.1 Houderschap en reikwijdte van het beleid 4

3.1.1 Identificatie bewerkersketen / begripsdefinities 5

3.1.2 IB beleid in de bewerkersketen 5

3.2 Uitwerking van dit beleid 6

3.3 Controle werking en naleving van het beleid 6

4 Beleidsuitgangspunten IB 7

5 Doelstellingen IB 9

1 Inleiding

Johan BV levert een SAAS oplossing (het “Johan Portaal”) waarmee bedrijven die aandacht willen besteden aan duurzame inzetbaarheid middels een partnerkanaal een scala aan (on- en offline) meetinstrumenten wordt geboden die het bedrijf in staat stellen de gezondheid en vitaliteit van hun medewerkers (voor de individuele medewerker) in kaart te brengen en deze middels diverse interventie programma’s te verbeteren.

Doordat Johan BV optreedt als (sub)bewerker in de zin van de AVG en het de ambitie van Johan BV is om optimale aandacht aan de beveiliging van persoonsgegevens te geven, stelt de directie zich op het standpunt dat ISO27001 certificering hiertoe noodzakelijk is. De VVT dient naast de van toepassing zijnde beheersmaatregelen uit appendix A van de norm (lees: ISO 27002) uit een aantal extra controls te bestaan, die specifiek de focus leggen op compliance met de AVG.

Daarnaast zijn hiaten in Informatiebeveiliging een groot bedrijfsrisico voor Johan BV, en is het dus noodzakelijk deze risico’s adequaat te beheersen. ISO27001 certificering dient de inspanningen van Johan op dit IB vlak aantoonbaar te maken.

2 Verantwoordelijkheid, doelstelling en doelgroep

Gelet op de mogelijke impact van verstoringen op de bedrijfsvoering en continuïteit van Johan BV en haar klanten berust eindverantwoordelijkheid voor het beleid inzake informatiebeveiliging bij de directie van Johan BV.

Het Beleidsdocument Informatiebeveiliging (hierna te noemen beleid IB) heeft als doel de risico’s m.b.t. de vertrouwelijkheid, integriteit en continuïteit van de informatievoorziening binnen Johan BV te beheersen en definiëren we als volgt:

> ‘*Het bieden van een raamwerk van beleidsuitgangspunten met betrekking tot de vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening, waarbinnen een evenwichtig (doeltreffend en doelmatig) stelsel van onderling samenhangende maatregelen ontwikkeld wordt, teneinde de informatievoorziening te beschermen tegen interne en externe bedreigingen’*.

Alle betrokkenen dienen ervoor zorg te dragen, dat aan de in dit beleid IB geformuleerde beleidsuitgangspunten wordt voldaan bij de inrichting van de organisatie, procedures, werkwijze en de daarbij gehanteerde informatiesystemen.

3 Toepassingsgebied

Dit beleid is van toepassing op alle informatie die gecreëerd, ontvangen, verzonden of bewaard wordt in de dienstverlening van Johan BV aan klanten en de daarmee samenhangende contractuele verplichtingen en ondersteunende processen. Het beleid en de uitwerking hiervan gelden voor alle medewerkers van Johan BV. Afwijkingen hierop moeten gemeld worden, zodat het management systeem continu verbeterd kan worden. Daarnaast geldt beleid ook voor contractanten, die Johan BV ondersteunen bij haar dienstverlening aan klanten.

Onlosmakelijk onderdeel van dit beleid is de ethische code, waaraan ook alle medewerkers, contractanten en stagiaires zich dienen te houden. Zoveel mogelijk wordt gestreefd naar het kiezen van beveiligingsmaatregelen gebaseerd op logische principes, omdat deze kosteneffectief en duurzaam zijn. Deze principes zijn:

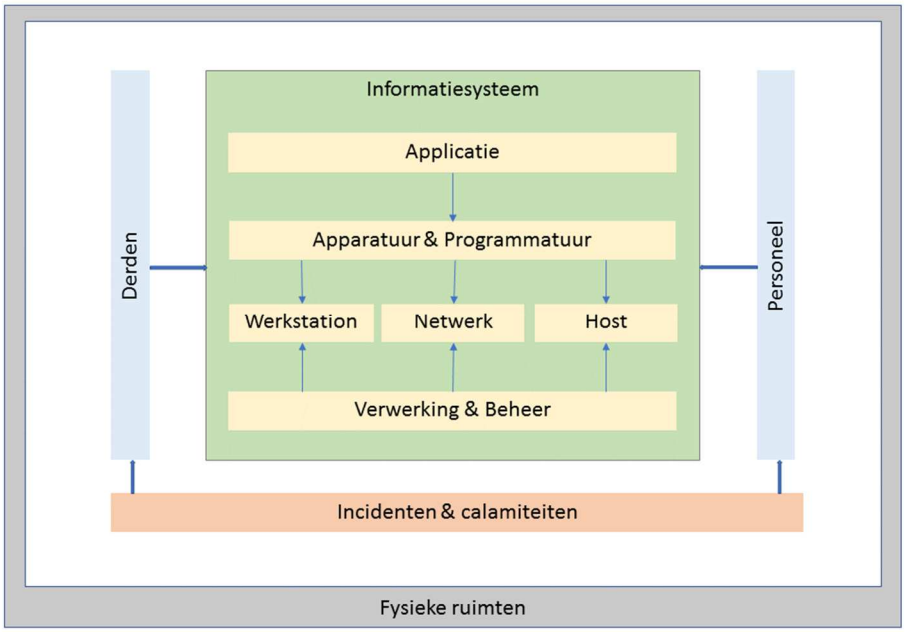
- Data, die je niet hebt of die niet vertrouwelijk zijn, hoef je ook niet te beveiligen;
- Niet slepen met informatie (dus niet kopiëren);
- Scheiden van informatie.

Alle medewerkers worden geacht deze principes in de praktijk te brengen.

3.1 Houderschap en reikwijdte van het beleid

Johan BV is dus verantwoordelijk voor het beschikbaar stellen van haar dienst met voldoende beveiligingsopties, zodat haar klanten kunnen voldoen aan de voor haar geldende IB-normen en andere wet- en regelgeving. Ook voldoet de hosting en het beheer van de software aan deze eisen. Dit ontslaat echter de klant niet van de eindverantwoordelijkheid voor de beveiliging van haar informatievoorziening.

Van elk informatiesysteem, inclusief de daarbij behorende gegevens, dient expliciet één houder te zijn benoemd. Het houderschap impliceert de eindverantwoordelijkheid voor het betreffende systeem, inclusief het bepalen van bij het systeem te onderkennen risico's, het classificeren van het systeem en de daarbij behorende gegevens en het (laten) ontwikkelen van adequate beveiligingsmiddelen en interne controlemaatregelen. Naast de applicatie betreft dit ook de juiste inzet van de infrastructurele componenten (werkstations, servers en het interne en externe netwerk), de juiste verwerking, het adequate beheer, het goed functioneren van het personeel, het maken van afspraken met derden, fysieke beveiliging en voorzieningen om incidenten en calamiteiten te voorkomen of af te handelen. In onderstaand figuur zijn alle genoemde deelgebieden van een informatiesysteem opgenomen.



Er wordt gesproken over eindverantwoordelijk omdat een aantal aspecten van het informatiesysteem uitbesteed worden aan andere houders zoals bijv. hostingpartij(en). Hierbij wordt niet een maximaal beveiligingsniveau nagestreefd, maar een optimaal niveau, zodat Johan BV haar diensten kan bieden tegen een acceptabele kosten.

3.1.1 Identificatie bewerkersketen / begripsdefinities

Johan BV distribueert de licenties voor het Johan Portaal via een partnerkanaal. De partners zorgen voor de inrichting van het portaal aan de klantzijde. De klant biedt het Johan Portaal vervolgens aan haar werknemers aan. Contentleveranciers leveren content voor de applicatie in de vorm van meetinstrumenten, vragenlijsten, interventieprogramma's, thematische documentatie etc.

In de gehele bewerkersketen zijn dus de volgende partijen te onderscheiden:

1. Johan BV: SAAS leverancier van het Johan Portaal;
2. Partners: Distributiekanaal van het Johan Portaal, geen eindgebruiker;
3. Klantmanager: werknemer in dienst van een partner, die verantwoordelijk is voor het beheer van de klanten (eindafnemers) die via deze partner toegang krijgen tot het Johan Portaal;
4. Klant (eindafnemers): Neemt het Johan Portaal af via de partner;
5. Werknemer: natuurlijk persoon in dienst bij de klant, gebruiker van het Johan Portaal; betrokkene in termen van de AVG;
6. Contentleveranciers: leveren onder eigen condities content aan, die binnen het Johan Portaal door werknemers gebruikt wordt. Contentleveranciers kunnen partners zijn, klanten of derden, zoals wetenschappelijke instituten; (opgemerkt wordt dat Johan zelf geen content levert: zij neemt bewust een onafhankelijke positie in en laat dit aspect aan de markt over.)
7. Consultants / Implementors, andere dan Johan BV: Leveren consultancy aan partners m.b.t. tot het gebruik en inrichting van het Johan Portaal. Zijn vaak ook Partner;
8. Professionals: derden die via het partnerkanaal en/of de klant worden ingehuurd om diensten te verlenen aan de Werknemer. (Coaches, loopbaanbegeleiders, psychologen, arbo-adviseurs etc.)

NB: Beleid is gericht op distributie via de partners; mocht Johan bij wijze van uitzondering rechtstreeks het Johan Portaal aan een klant (eindgebruiker) aanbieden, dan neemt zij tegelijkertijd de rol van partner / consultant op zich. Content loopt altijd via derden en wordt nooit direct via Johan afgenomen.

3.1.2 IB beleid in de bewerkersketen

De scope van IB beleid van Johan strekt zich in beginsel uit tot de ontwikkeling, hosting, support en het beheer van het Johan Portaal en de beschikbaarstelling en beveiliging daarvan tot aan het partner kanaal. De partners zijn verantwoordelijk voor het beheer van klantaccounts. Klanten (eindgebruikers) zijn verantwoordelijk voor de door hen ingevoerde (werknemers) data in het Johan Portaal. E.e.a. dient via bewerkersovereenkomsten en SLA's te worden geregeld. Hoewel Johan de scope van haar IB beleid beperkt tot datgene waar zij zelf expliciet invloed op uitoefent, is zij zich bewust van haar uitgangspunten zoals die zijn vermeld in paragraaf 4: ook als het IB beleid zich niet verder uitstrekt dan tot het partnerkanaal, streeft Johan ernaar om bij de development van het Johan Portaal dusdanig rekening te houden met "privacy-by-design" en "security-by-design" principes, dat de partners en klanten een optimaal veilige omgeving geboden wordt, die recht doet

aan de IB uitgangspunten. Daarbij stelt Johan BV eisen aan de partners en specifiek aan de klantmanagers en acht zij het van belang partners en klantmanagers te trainen opdat zij aan deze eisen kunnen voldoen.

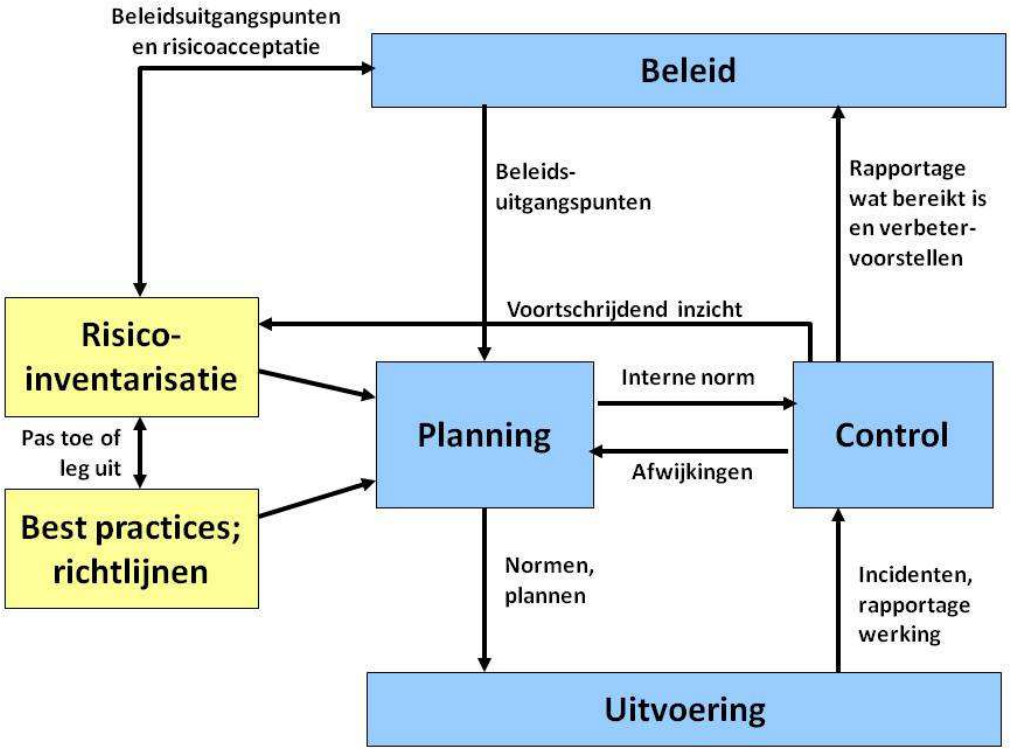
3.2 Uitwerking van dit beleid

Op basis van dit beleid worden risico analyses uitgevoerd en wordt een set van maatregelen en controls gedefinieerd als interne norm, dat geldt als minimum voor de dienstverlening aan klanten. Het document dat deze interne norm beschrijft, is daarom onlosmakelijk verbonden met dit beleid.

3.3 Controle werking en naleving van het beleid

In de directiebeoordeling wordt de werking en de naleving van het beleid intern geëvalueerd en zo nodig aangepast.

Minimaal tweejaarlijks wordt een interne audit gehouden en vaker indien er sprake is van significante wijzigingen in het beleid of de systemen waarop het beleid van toepassing is. Onderdeel van deze interne audit zijn het opnieuw beoordelen van risico's en een beoordeling van nieuwe contracten en wet- en regelgeving. Onderdeel van deze rapportage is ook een plan met verbetervoorstellen. De directie beoordeelt de rapportage, keurt voorstellen al dan niet goed en kent budget toe voor de realisatie van de voorstellen. Onderstaand is dit schematisch weergegeven.



Daarnaast wordt jaarlijks een audit uitgevoerd door een onafhankelijke derde partij, die hiertoe bevoegd en deskundig is. De rapportage hiervan is ter inzage beschikbaar voor (potentiële) klanten.

4 Beleidsuitgangspunten IB

Met onderstaande kwalitatieve beleidsuitgangspunten verwacht Johan B.V. haar informatie-beveiligingsrisico's te beheersen en tegelijk haar flexibiliteit en efficiency bij het uitvoeren van haar werkzaamheden te behouden.

De beleidsuitgangspunten vormen de brug tussen de informatiebeveiligingsrisico's en de beheersdoelstellingen en -maatregelen uit de Interne Norm van Johan B.V.

De beleidsuitgangspunten bieden bovendien het kader voor de directie, op welke wijze zij wil dat de informatiebeveiligingsdoelstellingen worden vormgegeven, die passend zijn voor Johan B.V. Genoemde beleidsuitgangspunten gelden voor die gegevensbewerkingen, waarvoor Johan B.V. wettelijk en/of contractueel verantwoordelijk is.

1. Informatiebeveiliging is een belangrijk bedrijfsrisico voor Johan B.V.. De directie stelt daarom het beleid vast, beoordeelt de risico's, stelt de maatregelen vast, stelt voldoende middelen ter beschikking en laat periodiek de werking van het beleid en de naleving van deze maatregelen intern en extern beoordelen om te borgen, dat het IB-managementsysteem blijvend adequaat werkt en waar nodig verbeterd wordt.
2. Johan B.V. conformeert zich m.b.t. de informatiebeveiliging aan de relevante wetgeving en de contractuele afspraken met klanten en business partners.
3. Johan B.V. streeft ernaar om haar dienstverlening aan klanten continu te verbeteren.
4. De beheersdoelstellingen en beheersmaatregelen van de norm NEN-ISO/IEC 27001 en de privacyrichtlijnen van de Autoriteit Persoonsgegevens (AP) vormen, voor zover zij bijdragen aan de informatiebeveiliging van Johan B.V. en handhaafbaar zijn, het uitgangspunt voor de te definiëren maatregelen. Dit is vooral een bedrijfseconomische afweging.
5. Johan B.V. beschouwt computercriminaliteit als een ongewenst maatschappelijk probleem en ziet het slechts als haar taak om passende maatregelen te nemen om schade ten gevolge van criminele activiteiten zoveel mogelijk te beperken.
6. Vertrouwen is voor Johan B.V. een groot goed en zij hanteert naar medewerkers, klanten, leveranciers en andere stakeholders het wederkerigheidsprincipe. Johan B.V. gaat ervan uit, dat zij afspraken nakomen m.b.t. beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening.
7. Het HRM-beleid is mede gericht op het verbeteren van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening bij medewerkers. Tijdens een jaarlijkse evaluatie wordt dit aan de orde gesteld.
8. De fysieke en logistieke beveiliging van de gebouwen en de ruimtes daarin zijn zodanig, dat de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens en gegevensverwerking inclusief de bedrijfsmiddelen gewaarborgd zijn.
9. Ontwikkeling of aanschaf, installatie en onderhoud van informatie- en communicatiesystemen, alsmede inpassing van nieuwe technologieën, moeten zo nodig met aanvullende maatregelen worden uitgevoerd, dat hiermee geen afbreuk wordt gedaan aan de informatiebeveiliging.

10. Opdrachten aan derden voor het uitvoeren van werkzaamheden worden zodanig omgeven met maatregelen, dat er geen inbreuk op de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening kan ontstaan.
11. Bij de verwerking en het gebruik van gegevens worden maatregelen getroffen om de privacy van klanten, medewerkers en andere betrokkenen te waarborgen.
12. Toegangsbeveiliging zorgt ervoor, dat ongeautoriseerde personen of processen geen toegang krijgen tot de informatiesystemen, gegevensbestanden en programmatuur van Johan B.V..
13. Gegevensverstrekking extern gebeurt op basis van 'need to know'. Intern is dit niet altijd wenselijk omdat kennisdeling essentieel is voor een kosteneffectieve dienstverlening aan klanten.
14. Johan B.V. en haar medewerkers treffen maatregelen om te voorkomen, dat vertrouwelijke informatie in handen van derden terechtkomt.
15. Input van klanten die vertrouwelijke data bevat, wordt na verwerking op korte termijn gearchiveerd of vernietigd.
16. Datatransport is zodanig met beveiligingsmaatregelen omkleed, dat geen inbreuk kan worden gepleegd op de vertrouwelijkheid en de integriteit van deze gegevens.
17. Geautoriseerde medewerkers moeten ook op afstand een beveiligde toegang hebben tot de voor hun relevante productie omgevingen. Er worden geen vertrouwelijke gegevens buiten de productieomgeving opgeslagen. Voor data die niet betrekking heeft op het Johan DI Portaal, kan hier onder condities van afgeweken worden.
18. Productie omgevingen zijn gescheiden van andere omgevingen en hierin kunnen specifiek toegangsrechten worden verleend en is monitoring van de toegang mogelijk.
19. Het beheer en de opslag van gegevens in productieomgevingen zijn zodanig, dat geen informatie verloren kan gaan tenzij er sprake is van overmacht.
20. Er zijn functiescheidingen aangebracht tussen de ontwikkel-, beheer- en gebruikersorganisatie. Verder wordt functiescheiding toegepast waar dat mogelijk en wenselijk is.
21. Er is een proces om incidenten adequaat af te handelen en hier 'lessons learned' uit te trekken.
22. Er zijn calamiteitenplannen en -voorzieningen om de beschikbaarheid van de informatievoorziening te waarborgen.
23. Bij uitbesteding van gegevensverwerking kan de directie besluiten om tijdelijk af te wijken van deze beleidsuitgangspunten en de risico's hiervan tijdelijk te accepteren.
24. Bij conflicten prevaleert de missie van Johan B.V. boven de eisen die gesteld worden door IB en of privacy.
25. Informatiebeveiliging is onderdeel van het ontwerpen, ontwikkelen en beheren van software, ook als die door derden wordt ontwikkeld. Security by design en privacy by design en default vormen hierbij de voornaamste uitgangspunten.
26. Johan B.V. en haar medewerkers realiseren zich de privacy gevoeligheid van de (bijzondere) persoonsgegevens die zij verwerken en waarborgen te allen tijde de afscherming, corrigeerbaarheid en transparantie van deze gegevens ter bescherming van de persoonlijke levenssfeer van de betrokkenen.

5 Doelstellingen IB

Bij genoemde uitgangspunten passen de volgende doelstellingen. Bij de uitwerking van het beleid dienen maatregelen geformuleerd te worden die het behalen van deze doelstellingen faciliteren. De doelstellingen zijn meetbaar. Minimaal vier maal per jaar controleert JOHAN of zij aan haar eigen doelstellingen voldoet.

1. Beschikbaarheid van het Johan Portaal op jaarbasis: minimaal 99,9% op jaarbasis en 99,5% op maandbasis, exclusief geplande downtime; niet meer dan 1 high impact verstoring (lees: ongeplande downtime voor langer dan 3 uur) per kwartaal.
2. Vertrouwelijkheid: Maximaal 1 onbevoegde toegang tot klantomgevingen per kwartaal toe te rekenen aan Johan BV.
3. Integriteit: Maximaal 1 melding per maand van een foutieve verwerking, toe te rekenen aan Johan BV.
4. Continue verbetering.
    a. Minimaal twee major releases per jaar
    b. Minimaal maandelijks minor releases met bugfixes e.d.
    c. Minimaal 3 geaccepteerde wijzigingen per maand
    d. 95% van de IB-incidenten wordt binnen een maand gesloten
5. Geen major afwijkingen bij externe audit; niet meer dan 3 minor afwijkingen