Johan

Beleid Informatiebeveiliging Johan BV

Opsteller: G. Westerlaken
Datum 1e versie: 01-11-2017
Laatste revisie: 02-08-2023
Status: definitief, goedgekeurd door directie.
Documentnaam: Beleid Informatiebeveiliging Johan BV.docx

Classificatie: openbaar.

Inhoud

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.

Het Portaal is een multi-tenant omgeving waarin uiteenlopende data van een groot aantal bedrijven en eindgebruikers is opgeslagen. In control zijn met betrekking tot informatiebeveiliging is daarom essentieel voor het vertrouwen dat gebruikers in het Portaal stellen. Doordat Johan BV optreedt als zowel verwerkingsverantwoordelijke als verwerker in de zin van de AVG en het de ambitie van Johan BV is om optimale aandacht aan gegevensbescherming en de beveiliging van persoonsgegevens, stelt de directie zich op het standpunt dat ISO27001 certificering hiertoe noodzakelijk is.
Niet alleen om in-control te zijn, maar ook om op een heldere manier verantwoording aan alle stakeholders af te kunnen leggen. De bijbehorende Verklaring Van Toepasselijkheid (VVT) dient naast de van toepassing zijnde beheersmaatregelen uit appendix A van de norm 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:

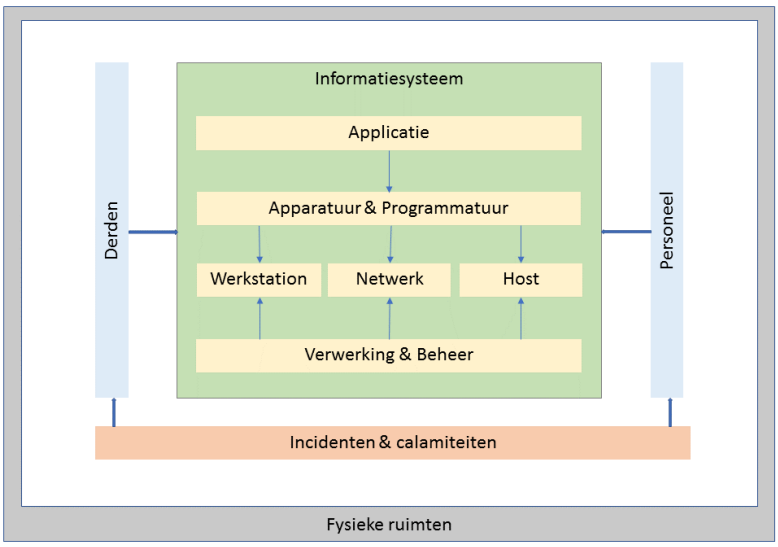
- Data, die je niet hebt of die niet vertrouwelijk zijn, hoef je ook niet te beveiligen;
- Niet slepen met informatie (dus niet kopiëren);
- Scheiden van informatie.

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

3.1 Houderschap en reikwijdte van het beleid

Johan BV is verantwoordelijk voor het beschikbaar stellen van haar dienst (het Johan Portaal) 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. Het optimale niveau is gebaseerd op de werkwijze zoals beschreven in paragraaf 3.2.

3.2 Uitwerking van dit beleid

Op basis van dit beleid en de beleidsuitgangspunten worden periodiek risico analyses uitgevoerd en wordt een set van maatregelen (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 en vormt een essentieel onderdeel van het ISMS. Bij het kiezen van maatregelen vormt de ISO27001 appendix een leidraad maar niet de enige bron waaruit maatregelen gekozen kunnen worden. De praktische uitwerking vindt plaats in het ISMS, dat het effect van PDCA cycli m.b.t. IB aantoonbaar maakt.

3.3 ISMS

Het beleid en de uitwerking hiervan wordt beheerd in het ISMS (Information Security Management System). Dit ISMS omvat onder meer:

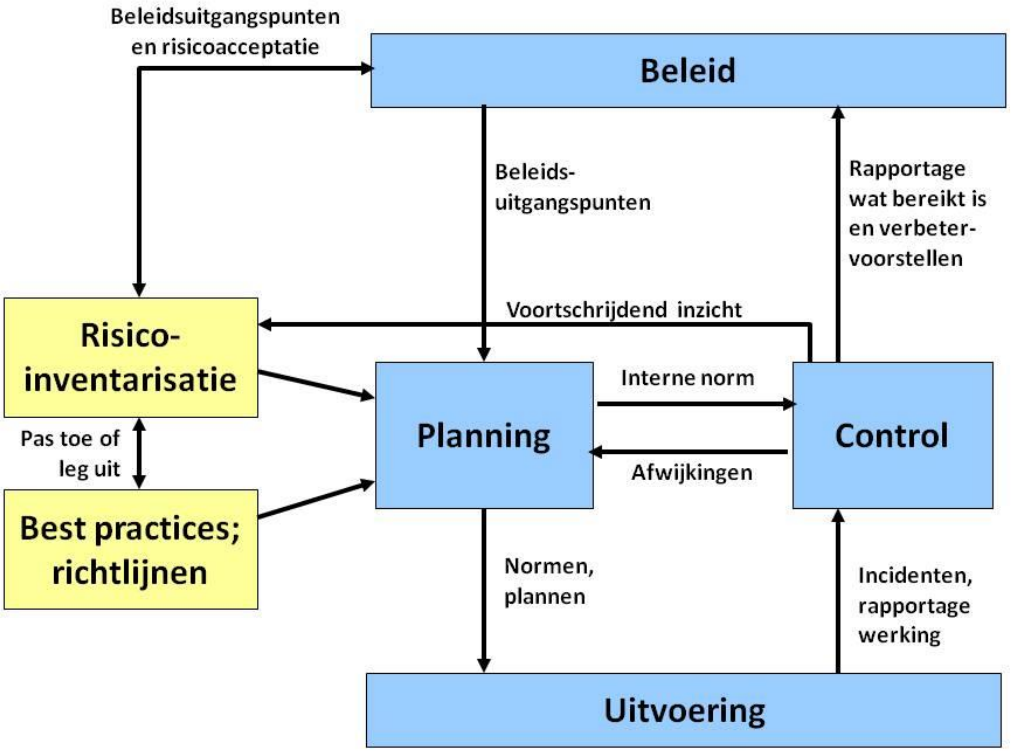
- De ISO27001 norm;
- Het IB beleid en de beleidsuitgangspunten;
- De resultaten van de periodiek uit te voeren risico-analyses inclusief een koppeling naar de beleidsuitgangspunten waar de risico's een bedreiging voor vormen;
- De maatregelen die geselecteerd worden om de risico's af te dekken;
- De uitwerking van de maatregelen in een interne norm;
- De verwijzingen naar bijbehorende documenten en procedures;
- De IB doelstellingen;

- De periodieke activiteiten en controles die noodzakelijk zijn om deze doelstellingen te bereiken, gevat in een operationele planning;
- Een verbeterplan, waarin de te verbeteren punten zijn opgenomen, inclusief de methode waarop deze te realiseren zijn, de benodigde resources en operationele planning voor het bewaken van de voortgang;
- De resultaten van audits en periodieke controle op het IB beleid en de werking van het ISMS.

3.4 Controle werking en naleving van het beleid

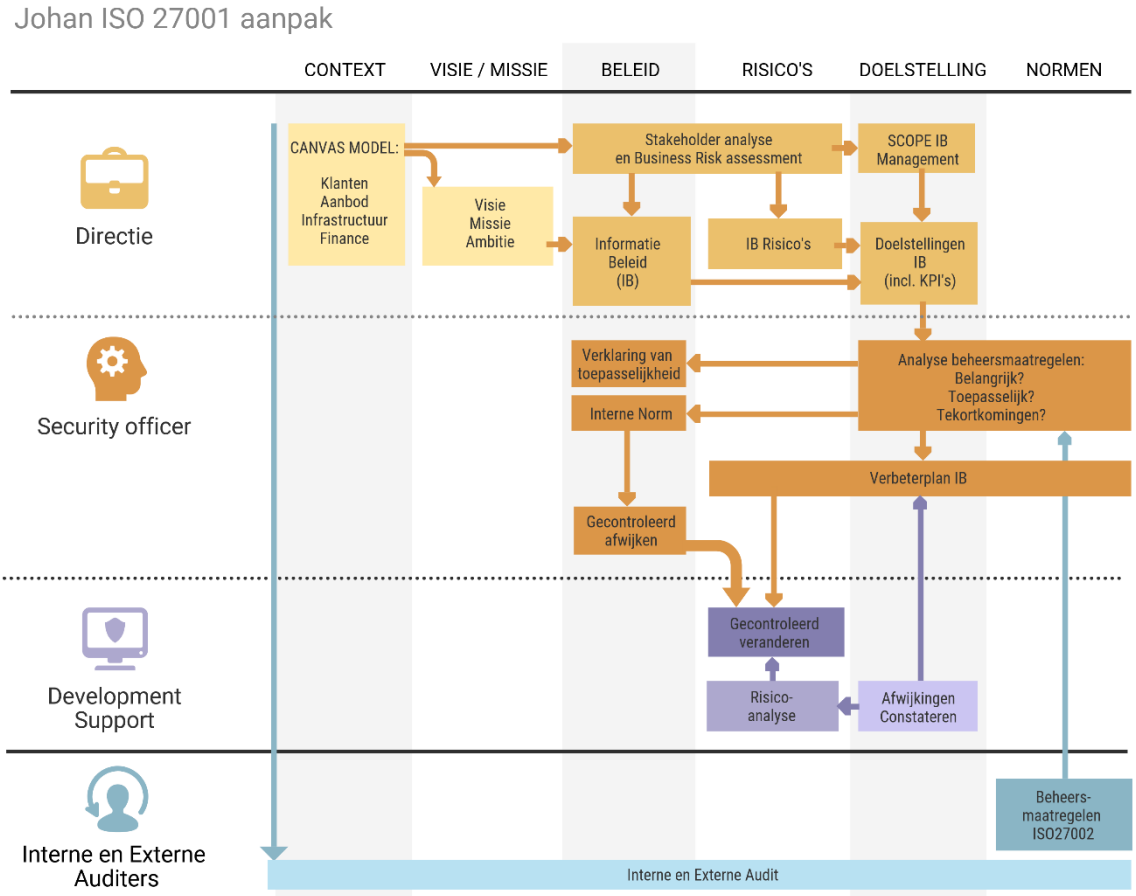
In de directiebeoordeling wordt de werking en de naleving van het beleid intern geëvalueerd en zo nodig aangepast.

Minimaal jaarlijks 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. E.e.a. is schematisch weergegeven in de volgende afbeelding:



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.

De rollen, verantwoordelijkheden en aandachtsgebieden zijn verder zichtbaar in onderstaande swimlane.



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 periodieke 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 principes 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 Relatie met beheersmaatregelen uit ISO 27002

Hieronder staan implementatierichtlijnen voor verdere beleidsontwikkeling ten aanzien van een aantal maatregelen uit de ISO-27002 norm.

5.1 Toegangsbeveiliging

Toegangsbeveiliging zorgt ervoor, dat ongeautoriseerde personen of processen geen toegang krijgen tot de informatiesystemen, gegevensbestanden en programmatuur van Johan B.V.. Bij de maatregelen voor logische toegangsbeveiliging wordt specifiek gelet op de aard van de te beschermen informatie en het belang daarvoor voor de organisatie of externe stakeholders. Daar waar het belang groot is en/of informatie als hoog vertrouwelijk is geclassificeerd, wordt zoveel mogelijk gebruik gemaakt van multiple factor authenticatie. Medewerkers dienen bekend te zijn met de praktische richtlijnen m.b.t. logische toegangsbeveiliging en hier naar te handelen.

Zie ook hfst. 9 ISO-27002

5.2 Classificatie van informatie

Informatie wordt geclassificeerd in vier oplopende classificatieniveaus: Geen (volledig openbaar), Laag (intern openbaar), Middel (intern vertrouwelijk), Hoog (strikt vertrouwelijk). Het classificatieschema is uitgewerkt in het personeelshandboek. Medewerkers dienen bekend te zijn met de praktische richtlijnen m.b.t. classificatie en hier naar te handelen.

Zie ook hfst. 8.2 ISO-27002

5.3 Fysieke en omgevingsbeveiliging

Kantoorgebouwen van Johan zijn afdoende beveiligd tegen inbraak. Beleid moet er op gericht zijn, om de gevolgschade t.g.v. inbraak, brand of waterschade als restrisico te kunnen accepteren. Dit wordt o.a. gerealiseerd door een clear screen en clear desk policy en vertrouwelijk geclassificeerde data zo min mogelijk op papier te archiveren. Medewerkers dienen altijd thuis te kunnen werken, teneinde de afhankelijkheid van een kantoorpand verder te verkleinen.

Johan is zelf onvoldoende bij machte om de fysieke veiligheid die nodig is voor hosting, in haar eigen kantoorpand te waarborgen. Data wordt dus nooit op het kantoorpand gehost, maar altijd in een goed afgeschermd datacenter.

Zie ook hfst. 11 ISO-27002

5.4 Onderwerpen die gericht zijn op de eindgebruiker c.q. medewerker

1) aanvaardbaar gebruik van bedrijfsmiddelen (Hfst. 8.1.3 ISO-27002)
Aanvaardbaar gebruik van bedrijfsmiddelen is vooral gericht op de toepassing van de “Ethische Code” van Johan. Medewerkers tekenen hiervoor. Uitwerking vindt plaats in het personeelshandboek.

2) ‘Clear Desk’ en ‘Clear Screen’ (Hfdst. 11.2.9 ISO-27002)

IB risico's worden sterk gereduceerd als iedere medewerker consequent de 'clear desk' en 'clear screen' policy hanteert. Medewerkers snappen dit en passen dit als een vanzelfsprekendheid toe.

3) Informatietransport (Hfdst. 13.2.1 ISO-27002);

Medewerkers van Johan zijn zich bewust van de classificatie van informatie. Aan de hand van deze classificatie nemen zij passende maatregelen om deze informatie te beveiligen wanneer die intern of extern wordt uitgewisseld.

4) mobiele apparatuur en telewerken (Hfdst. 6.2 ISO-27002);

De "ethische Code" is van toepassing op het gebruik van mobiele apparatuur. Johan vindt het van groot belang dat iedereen net zo eenvoudig thuis kan werken als op kantoor. Uitgangspunt van de kantoorautomatisering is dan ook, dat er zoveel mogelijk gebruik gemaakt wordt van SaaS applicaties, opdat medewerkers voldoende hebben aan een recente Internet browser om al hun werkzaamheden te kunnen doen.

5) beperkingen t.a.v. software-installaties en -gebruik (Hfdst. 12.6.2 ISO-27002);

Door zoveel mogelijk gebruik te maken van SaaS applicaties kan het aantal applicaties op PC's en laptops beperkt worden en is het toepassen van beperking t.a.v. software-installaties eenvoudiger te implementeren in de praktijk.

6) Zorgdragen voor veilig personeel (Hfdst. 7 ISO-27002)

Johan stelt zich op het standpunt dat medewerkers worden gescreend, voorafgaand aan in-dienst treding. Voor hen met toegang tot het Johan Portaal is een VOG verklaring vereist.

5.5 Back-up

Binnen de SaaS toepassingen van de kantoorautomatisering zijn back-ups een uitbesteed proces. Leveranciers van SaaS oplossingen dienen om die reden een hoge beschikbaarheid te kunnen garanderen. Het backup plan van de data in het Johan Portaal dient minimaal een 3-2-1 schema te volgen met een RTO / RPO die minimaal overeenkomstig is met gangbare eisen vanuit de markt.

Zie ook hfdst. 12.3 ISO-27002

5.6 Informatietransport

Datatransport is zodanig met beveiligingsmaatregelen omkleed, dat geen inbreuk kan worden gepleegd op de vertrouwelijkheid en de integriteit van deze gegevens.

Zie ook hfdst. 13.2 ISO-27002

5.7 Bescherming tegen malware

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. Het gaat hierbij niet alleen om "best practices" als encryptie, beperken van administrator rechten en toepassingen van anti-malware software. Medewerkers worden ook geacht hier een actieve rol in te spelen, bijvoorbeeld doordat zij weten hoe zij phishing en social engineering kunnen herkennen en weten hoe daar op te reageren.

Zie ook hfdst. 12.2 ISO-27002

5.8 Beheer van technische kwetsbaarheden

Het beheer en de opslag van gegevens in productieomgevingen zijn zodanig, dat geen informatie verloren kan gaan tenzij er sprake is van overmacht. Een passend patch beleid is hierbij nodig om de risico's van technische kwetsbaarheden te beheersen.

Zie ook hfdst. 12.6.1 ISO-27002);

5.9 Cryptografische beheersmaatregelen

Bij het toepassen ban crypografische beheersmaatregelen wordt altijd rekening gehouden met de volgende uitgangspunten: welke maatregelen worden genomen is afhankelijk van het toepassingsgebied en de classificatie van de informatie; er is sprake van proportionele toepassing; cryptografische beheersmaatregelen moeten een passend beveiligingsniveau waarborgen; er wordt gebruik gemaakt van bewezen techniek en open standaarden.

Zie ook hfdst. 10 ISO-27002

5.10 Communicatiebeveiliging

Netwerken moeten worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen. Risico's bij uitbestede netwerkdiensten, zoals de hosting van het Johan Portaal, dienen te worden beheerd door onder meer afgegeven SLA's (die voldoen aan de IB eisen van Johan) en het recht op audit.

Zie ook hfdst. 13 ISO-27002

5.11 Privacy en bescherming van persoonsgegevens

Privacy is een groot goed; gegevensbescherming is dan ook noodzaak. Johan committeert zich aan de AVG en neemt hiervoor extra maatregelen op in haar ISO-27001 Verklaring van Toepasselijkheid (VVT). Privacy by design en default principes vormen hierbij de voornaamste uitgangspunten.

Zie ook hfdst. 18.1.4 ISO-27002

5.12 Leveranciersrelaties

Leveranciers met toegang tot bedrijfsmiddelen van de organisatie worden opgenomen in het leveranciersoverzicht en periodiek beoordeeld. De eisen die gesteld worden aan de leveranciers in combinatie met de periodieke beoordeling vormt de basis voor het leveranciersmanagement. Relevante certificering van de leverancier en/of contractuele afspraken omtrent informatiebeveiliging vormt de relevante basis voor naleving. De directie bepaalt welke IB van toepassing zijn voor welke leveranciers. De directie wordt actief betrokken bij de keuze van leveranciers voor wie toegang tot bedrijfsmiddelen van de organisatie noodzakelijk is. De directie maakt de uiteindelijke keuze en is daarvoor verantwoordelijk.

Zie ook hfdst. 15 ISO-27002

5.13 Beleid voor veilig ontwikkelen van software

De ontwikkeling van de software van het Johan Portaal is zodanig met maatregelen omgeven, dat deze geen bedreiging vormt voor de hoog-hoog-hoog BIV classificatie van het Johan Portaal. Dit omvat onder meer: beleid voor de Secure Software Development Lifecycle, gebaseerd op toepassing van diverse best-practices; gebruik maken van de laatste versies van standaard ontwikkeltalen; toepassing van broncode beheer; toepassing strikt logisch en fysiek gescheiden OTAP straat; commitment aan de OWASP top tien; toepassing testprocedures; gedocumenteerde release procedure; periodieke PEN testen; toepassing van een PDCA cycli; toepassing incidentbeheer en wijzigingsprocedure.

6 Baseline Informatiebeveiliging Overheid

Bij het kiezen van maatregelen en het bepalen van gewenste niveaus van informatiebeveiliging richt Johan zich op richtlijnen van de “Baseline Informatiebeveiliging Overheid” (BIO) en die van het “Centrum Informatiebeveiliging en Privacybescherming”(CIP).

7 Doelstellingen IB

Op basis van de genoemde uitgangspunten worden interne en externe doelstellingen geformuleerd. Bij de uitwerking van het beleid dienen maatregelen geformuleerd te worden die het behalen van deze doelstellingen faciliteren. De doelstellingen zijn meetbaar en voldoen aan het SMART principe. Periodiek, doch minimaal tweemaal per jaar controleert JOHAN of zij aan haar eigen doelstellingen voldoet.

De doelstellingen zijn benoemd in een apart document en zijn op verzoek ter inzage. Doelstellingen die binnen het kader van de dienstverlening aan de klant van belang zijn voor de klant, worden benoemd in de SLA's die Johan met haar klanten afsluit. (Denk bijv. aan doelstellingen m.b.t. beschikbaarheid en response- en oplostijden.)

8 Bijlage: Overzicht ISO-27001 Documenten

Documenten per normhoofdstuk

Onderstaande tabel geeft een overzicht van de door Johan opgestelde en beheerde documenten binnen het ISMS. De documenten zijn een uitwerking van de beleidsuitgangspunten, waarin de informatiebeveiligingseisen en procedures zijn geformuleerd.

Als “intern” geclassificeerde documenten kunnen op verzoek worden ingezien; toestemming hiervoor is nodig vanuit de security officer.

Hfdstk	Naam Hoofdstuk	Omschrijving	Classificatie[1]
4.1	Inzicht verkrijgen in de organisatie en haar context	Hoofdlijnendocument JOHAN	Openbaar
4.2	Inzicht verkrijgen in behoeften en verwachtingen van belanghebbenden	Hoofdlijnendocument JOHAN	Openbaar
4.3	Toepassingsgebied van het ISMS vaststellen	Hoofdlijnendocument JOHAN	Openbaar
5.1	Leiderschap en betrokkenheid	Beleid Informatiebeveiliging Johan	Openbaar
5.1	Leiderschap en betrokkenheid	Informatiebeveiligingsdoelstellingen Johan	Intern
5.1	Leiderschap en betrokkenheid	Monitoren, Meten, Analyseren Evalueren ISMS	Intern
5.1	Leiderschap en betrokkenheid	Organisatie IB Johan	Intern
5.1	Leiderschap en betrokkenheid	Procedure Incident-probleem beheer en IC – Johan BV	Intern
5.1	Leiderschap en betrokkenheid	Procedure Wijzigingsbeheer Johan	Intern
5.2	Beleid	Beleid Informatiebeveiliging Johan	Openbaar
5.2	Beleid	JOHAN Portaal – Eigenaarschap van data, borging privacy en de AVG	Openbaar
5.3	Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie	Organisatie IB Johan	Intern
6.1	Maatregelen om risico’s te beperken en kansen te benutten	Risico assessment en behandel methodiek Johan	Intern
6.1.1	Algemeen	Risico assessment en behandel methodiek Johan	Intern
6.1.2	Risicobeoordeling van informatiebeveiliging	Risico assessment en behandel methodiek Johan	Intern
6.1.3	Behandeling van informatiebeveiligingsrisico’s	Risico assessment en behandel methodiek Johan	Intern
6.1.3	Behandeling van informatiebeveiligingsrisico’s	Verklaring van Toepasselijkheid ISO27001 Johan BV	Openbaar
6.2	Informatiebeveiligingsdoelstellingen en de planning om ze te bereiken	Informatiebeveiligingsdoelstellingen Johan	Intern
6.2	Informatiebeveiligingsdoelstellingen en de planning om ze te bereiken	Monitoren, Meten, Analyseren Evalueren ISMS	Intern
7.2	Competentie	Johan Personeelshandboek	Intern
7.2	Competentie	Personeelshandboek Johan	Intern
7.2	Competentie	Vakbekwaamheid medewerkers Johan – Competentiematrix	Intern
7.3	Bewustzijn	Communicatieplan IB	Intern
7.4	Communicatie	Communicatieplan IB	Intern
7.4	Communicatie	Procedure beheer van documenten – Johan	Intern
7.5.1	Gedocumenteerde informatie – Algemeen	Procedure beheer van documenten – Johan	Intern

[1] De classificatie “Intern” verwijst naar documenten die in de interne organisatie van Johan BV als “intern openbaar” zijn geclassificeerd. Omwille van de leesbaarheid is dat hier afgekort als “intern”.

7.5.1	Gedocumenteerde informatie - Algemeen	Relatie tussen de ISO 27001 norm en de IB documenten	Intern
7.5.3	Beheer van gedocumenteerde informatie	Procedure beheer van documenten - Johan	Intern
8.1	Operationele planning en beheersing	Hoofdlijnendocument JOHAN	Openbaar
8.1	Operationele planning en beheersing	Leverancier overzicht IB	Intern
8.1	Operationele planning en beheersing	Leveranciersrelaties Johan - Beleidsuitgangspunten	Intern
8.1	Operationele planning en beheersing	Procedure operationele planning IB Johan	Intern
8.2	Risicobeoordeling van informatiebeveiliging	Risico assessment en behandel methodiek Johan	Intern
9.1	Evaluatie: Monitoren, meten, analyseren en evalueren	Monitoren, Meten, Analyseren Evalueren ISMS	Intern
9.2	Evaluatie: Interne Audit	Auditplan Johan	Intern
9.3	Evaluatie: Directiebeoordeling	Directiebeoordeling IB Johan BV	Intern
10.1	Afwijkingen en corrigerende maatregelen	Procedure Incident-probleem beheer en IC - Johan BV	Intern
10.1	Afwijkingen en corrigerende maatregelen	Procedure Wijzigingsbeheer Johan	Intern

Documenten behorende bij maatregelen uit appendix A

Onderstaande overzicht is een cross-referentie van interne documenten en de maatregelen uit o.a. appendix A van de ISO-27001 norm.

Als “intern” geclassificeerde documenten kunnen op verzoek worden ingezien; toestemming hiervoor is nodig vanuit de security officer.

Maatregel	Omschrijving maatregel	Documentnaam
A.5.1.1	Beleidsregels voor IB	Beleid Informatiebeveiliging Johan
A.5.1.1	Beleidsregels voor IB	Communicatieplan IB
A.5.1.2	Beoordelen van het IB-beleid	Auditplan Johan
A.5.1.2	Beoordelen van het IB-beleid	Directiebeoordeling IB Johan BV
A.6.1.1	Rollen en verantwoordelijkheden IB	Organisatie IB Johan
A.6.1.1	Rollen en verantwoordelijkheden IB	Vakbekwaamheid medewerkers Johan
A.6.1.1	Rollen en verantwoordelijkheden IB	Vakbekwaamheid medewerkers Johan - Competentiematrix
A.6.1.2	Scheiding van taken	Organisatie IB Johan
A.6.1.2	Scheiding van taken	Technische beschrijving en security aspecten Johan Portaal
A.6.1.3	Contact met overheidsinstanties	AP - aanmelding Functionaris Gegevensbescherming
A.6.1.3	Contact met overheidsinstanties	Communicatieplan IB
A.6.1.3	Contact met overheidsinstanties	JOHAN Portaal - Eigenaarschap van data, borging privacy en de AVG
A.6.1.3	Contact met overheidsinstanties	Meldingsformulier AP (Autoriteit Persoonsgegevens)
A.6.1.4	Contact met speciale belangengroepen	Belangengroepen IB en privacy
A.6.1.5	IB in projectbeheer	Procedure Incident-probleem beheer en IC - Johan BV
A.6.1.5	IB in projectbeheer	Procedure Wijzigingsbeheer Johan
A.6.2.1	Beleid voor mobiele apparatuur	Beveiliging van (mobiele) apparatuur
A.6.2.1	Beleid voor mobiele apparatuur	Cryptografische beheersmaatregelen beleid
A.6.2.1	Beleid voor mobiele apparatuur	Ethische code Johan BV
A.6.2.2	Telewerken	Richtlijnen voor thuis- en telewerken
A.7.1.1	Screening	Johan Personeelshandboek

A.7.1.1	Screening	Procedure medewerkers instroom - uitstroom
A.7.1.2	Arbeidsvoorwaarden	Checklist JOHAN In dienst
A.7.1.2	Arbeidsvoorwaarden	Ethische code Johan BV
A.7.1.2	Arbeidsvoorwaarden	Johan Personeelshandboek
A.7.1.2	Arbeidsvoorwaarden	Procedure medewerkers instroom - uitstroom
A.7.2.1	Directieverantwoordelijkheden	Beleid Informatiebeveiliging Johan
A.7.2.2	Bewustzijn, opleiding en training ten aanzien van IB	Informatiebeveiliging en privacy toets Johan
A.7.2.3	Disciplinaire procedure	Johan Personeelshandboek
A.7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	Checklist JOHAN uit-dienst
A.7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	Johan Personeelshandboek
A.7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	Procedure medewerkers instroom - uitstroom
A.8.1.1	Inventariseren van bedrijfsmiddelen	Bedrijfsmiddelen Johan BV
A.8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	Beveiliging van (mobiele) apparatuur
A.8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	Ethische code Johan BV
A.8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	Johan Personeelshandboek
A.8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	Procedure Toegangsbeveiliging Johan BV
A.8.1.4	Teruggeven van bedrijfsmiddelen	Johan Personeelshandboek
A.8.1.4	Teruggeven van bedrijfsmiddelen	Procedure medewerkers instroom - uitstroom
A.8.2.1	Classificatie van informatie	Johan Personeelshandboek
A.8.2.1	Classificatie van informatie	Procedure beheer van documenten - Johan
A.8.2.2	Informatie labelen	Procedure beheer van documenten - Johan
A.8.2.3	Behandelen van bedrijfsmiddelen	Johan Personeelshandboek
A.9.1.1	Beleid voor toegangsbeveiliging	Procedure Toegangsbeveiliging Johan BV
A.9.1.2	Toegang tot netwerken en netwerkdiensten	Procedure Toegang tot netwerken en netwerkdiensten
A.9.2.1	Registratie en uitschrijving van gebruikers	Checklist JOHAN In dienst
A.9.2.1	Registratie en uitschrijving van gebruikers	Checklist JOHAN uit-dienst
A.9.2.1	Registratie en uitschrijving van gebruikers	Procedure medewerkers instroom - uitstroom
A.9.2.1	Registratie en uitschrijving van gebruikers	Procedure Toegangsbeveiliging Johan BV
A.9.2.2	Gebruikers toegang verlenen	Autorisatiematrix Johan
A.9.2.2	Gebruikers toegang verlenen	Autorisatiematrix Johan - procedure
A.9.2.2	Gebruikers toegang verlenen	Procedure Identificatie procesflow
A.9.2.2	Gebruikers toegang verlenen	Procedure medewerkers instroom - uitstroom
A.9.2.2	Gebruikers toegang verlenen	Procedure Toegangsbeveiliging Johan BV
A.9.2.3	Beheren van speciale toegangsrechten	Autorisatiematrix Johan
A.9.2.3	Beheren van speciale toegangsrechten	Procedure Toegang tot netwerken en netwerkdiensten
A.9.2.3	Beheren van speciale toegangsrechten	Procedure Toegangsbeveiliging Johan BV
A.9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	Procedure Toegangsbeveiliging Johan BV
A.9.2.5	Beoordeling van toegangsrechten van gebruikers	Procedure medewerkers instroom - uitstroom
A.9.2.5	Beoordeling van toegangsrechten van gebruikers	Procedure Toegangsbeveiliging Johan BV
A.9.2.6	Toegangsrechten intrekken of aanpassen	Procedure medewerkers instroom - uitstroom
A.9.3.1	Geheime authenticatie-informatie gebruiken	Autorisatiematrix Johan - procedure
A.9.3.1	Geheime authenticatie-informatie gebruiken	Ethische code Johan BV
A.9.3.1	Geheime authenticatie-informatie gebruiken	Procedure Toegangsbeveiliging Johan BV

A.9.4.1	Beperking toegang tot informatie	Autorisatiematrix Johan
A.9.4.1	Beperking toegang tot informatie	Autorisatiematrix Johan - procedure
A.9.4.1	Beperking toegang tot informatie	Procedure Toegangsbeveiliging Johan BV
A.9.4.2	Beveiligde inlogprocedures	Procedure Toegangsbeveiliging Johan BV
A.9.4.2	Beveiligde inlogprocedures	Twee-factor authenticatie in het JOHAN Portaal
A.9.4.3	Systeem voor wachtwoordbeheer	Procedure Toegangsbeveiliging Johan BV
A.9.4.3	Systeem voor wachtwoordbeheer	Twee-factor authenticatie in het JOHAN Portaal
A.10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	Cryptografische beheersmaatregelen beleid
A.10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	Technische beschrijving en security aspecten Johan Portaal
A.10.1.2	Sleutelbeheer	Cryptografische beheersmaatregelen beleid
A.11.2.5	Verwijdering van bedrijfsmiddelen	Beveiliging van (mobiele) apparatuur
A.11.2.5	Verwijdering van bedrijfsmiddelen	Ethische code Johan BV
A.11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	Beveiliging van (mobiele) apparatuur
A.11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	Richtlijnen voor thuis- en telewerken
A.11.2.7	Veilig verwijderen of hergebruiken van apparatuur	Ethische code Johan BV
A.11.2.8	Onbeheerde gebruikersapparatuur	Beveiliging van (mobiele) apparatuur
A.11.2.8	Onbeheerde gebruikersapparatuur	Johan Personeelshandboek
A.11.2.9	'Clear desk'- en 'clear screen'-beleid	Beveiliging van (mobiele) apparatuur
A.11.2.9	'Clear desk'- en 'clear screen'-beleid	Johan Personeelshandboek
A.12.1.1	Gedocumenteerde bedieningsprocedures	Relatie tussen de ISO 27001 norm en de IB documenten
A.12.1.2	Wijzigingsbeheer	Git branching model
A.12.1.2	Wijzigingsbeheer	Procedure Wijzigingsbeheer Johan
A.12.2.1	Beheersmaatregelen tegen malware	Beveiliging van (mobiele) apparatuur
A.12.2.1	Beheersmaatregelen tegen malware	Richtlijnen voor het veilig gebruik van Internet en email
A.12.2.1	Beheersmaatregelen tegen malware	Technische beschrijving en security aspecten Johan Portaal
A.12.3.1	Back-up van informatie	Backup en Restore procedure Johan Portaal
A.12.5.1	Software installeren op operationele systemen	Procedure Wijzigingsbeheer Johan
A.12.6.1	Beheer van technische kwetsbaarheden	Procedure Incident-probleem beheer en IC - Johan BV
A.12.6.1	Beheer van technische kwetsbaarheden	Procedure Wijzigingsbeheer Johan
A.12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen	PEN Test Overeenkomst en vrijwaringsverklaring
A.13.1.2	Beveiliging van netwerkdiensten	Cryptografische beheersmaatregelen beleid
A.13.1.3	Scheiding in netwerken	Application Security Model
A.13.1.3	Scheiding in netwerken	Procedure Toegang tot netwerken en netwerkdiensten
A.13.2.1	Beleid en procedures voor informatietransport	Cryptografische beheersmaatregelen beleid
A.13.2.1	Beleid en procedures voor informatietransport	Johan Personeelshandboek
A.13.2.1	Beleid en procedures voor informatietransport	Procedure beheer van documenten - Johan
A.13.2.1	Beleid en procedures voor informatietransport	Procedure bewaartermijnen Johan
A.13.2.1	Beleid en procedures voor informatietransport	Richtlijnen voor het veilig gebruik van Internet en email
A.13.2.3	Elektronische berichten	Cryptografische beheersmaatregelen beleid
A.13.2.4	Vertrouwelijkheids- of geheimhoudings-overeenkomst	Ethische code Johan BV
A.13.2.4	Vertrouwelijkheids- of geheimhoudings-overeenkomst	Johan Personeelshandboek
A.13.2.4	Vertrouwelijkheids- of geheimhoudings-overeenkomst	Procedure medewerkers instroom - uitstroom
A.14.1.1	Analyse en specificatie van IB-eisen	Leveranciersrelaties Johan - Beleidsuitgangspunten

A.14.1.1	Analyse en specificatie van IB-eisen	Specificatie van informatiebeveiligingseisen
A.14.1.1	Analyse en specificatie van IB-eisen	Technische beschrijving en security aspecten Johan Portaal
A.14.1.2	Toepassingsdiensten op openbare netwerken beveiligen	Specificatie van informatiebeveiligingseisen
A.14.1.3	Transacties van toepassingsdiensten beschermen	Specificatie van informatiebeveiligingseisen
A.14.2.1	Beleid voor beveiligd ontwikkelen	Beveiligingsnormen voor systeem- en applicatie-ontwikkeling
A.14.2.1	Beleid voor beveiligd ontwikkelen	Countermeasures against specific threats in sofware development
A.14.2.1	Beleid voor beveiligd ontwikkelen	Specificatie van informatiebeveiligingseisen
A.14.2.1	Beleid voor beveiligd ontwikkelen	Technische beschrijving en security aspecten Johan Portaal
A.14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen	Beveiligingsnormen voor systeem- en applicatie-ontwikkeling
A.14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen	Procedure Wijzigingsbeheer Johan
A.14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen	Specificatie van informatiebeveiligingseisen
A.14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen	Technische beschrijving en security aspecten Johan Portaal
A.14.2.5	Principes voor engineering van beveiligde systemen	Beveiligingsnormen voor systeem- en applicatie-ontwikkeling
A.14.2.5	Principes voor engineering van beveiligde systemen	Countermeasures against specific threats in sofware development
A.14.2.5	Principes voor engineering van beveiligde systemen	Technische beschrijving en security aspecten Johan Portaal
A.14.2.6	Beveiligde ontwikkelomgeving	Beveiligingsnormen voor systeem- en applicatie-ontwikkeling
A.14.2.6	Beveiligde ontwikkelomgeving	Specificatie van informatiebeveiligingseisen
A.14.2.7	Uitbestede softwareontwikkeling	Beveiligingsnormen voor systeem- en applicatie-ontwikkeling
A.14.2.7	Uitbestede softwareontwikkeling	Specificatie van informatiebeveiligingseisen
A.14.2.8	Testen van systeembeveiliging	Functie en werkwijzen Testwerkzaamheden
A.14.2.8	Testen van systeembeveiliging	Procedure Wijzigingsbeheer Johan
A.14.2.8	Testen van systeembeveiliging	Specificatie van informatiebeveiligingseisen
A.14.2.9	Systeemacceptatie-tests	Specificatie van informatiebeveiligingseisen
A.14.3.1	Bescherming van testgegevens	Specificatie van informatiebeveiligingseisen
A.15.1.1	IB-beleid voor leveranciersrelaties	Leveranciersrelaties Johan - Beleidsuitgangspunten
A.15.1.2	Opnemen van beveiligingsaspecten in leveranciers-overeenkomsten	Verwerkersovereenkomst True Hosting
A.15.1.3	Toeleveringsketen van informatie- en communicatie-technologie	Leveranciersrelaties Johan - Beleidsuitgangspunten
A.15.1.3	Toeleveringsketen van informatie- en communicatie-technologie	Verwerkersovereenkomst True Hosting
A.15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	Leverancier overzicht IB
A.15.2.2	Beheer van veranderingen in de dienstverlening van leveranciers	Leveranciersrelaties Johan - Beleidsuitgangspunten
A.15.2.2	Beheer van veranderingen in de dienstverlening van leveranciers	Procedure Wijzigingsbeheer Johan
A.16.1.1	Verantwoordelijkheden en procedures	AP - aanmelding Functionaris Gegevensbescherming
A.16.1.1	Verantwoordelijkheden en procedures	Procedure Incident-probleem beheer en IC - Johan BV
A.16.1.2	Rapportage van IB-gebeurtenissen	Hoofdovereenkomst Johan (Licentie/SLA/Verwerksovereenkomst)
A.16.1.2	Rapportage van IB-gebeurtenissen	Procedure Incident-probleem beheer en IC - Johan BV
A.16.1.3	Rapportage van zwakke plekken in de IB	Johan Personeelshandboek
A.16.1.4	Beoordeling van en besluitvorming over IB-gebeurtenissen	Procedure Incident-probleem beheer en IC - Johan BV
A.16.1.5	Respons op IB-incidenten	Procedure Incident-probleem beheer en IC - Johan BV
A.17.1.1	IB-continuïteit plannen	Continuiteitsplan Johan BV

A.17.1.2	IB-continuïteit implementeren	Continuiteit advies Johan BV
A.17.1.2	IB-continuïteit implementeren	Continuiteitsplan Johan BV
A.18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen	Controller to Controller Overeenkomst
A.18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen	Hoofdovereenkomst Johan (Licentie/SLA/Verwerksovereenkomst)
A.18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen	JOHAN Portaal - Eigenaarschap van data, borging privacy en de AVG
A.18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen	Verwerkersovereenkomst tot gezamenlijke verwerkingverantwoordelijkheid
A.18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen	Welke wetgeving is wel en niet van toepassing op het Johan Portaal?
A.18.1.2	Intellectuele eigendomsrechten	Leveranciersrelaties Johan - Beleidsuitgangspunten
A.18.1.3	Beschermen van registraties	Procedure beschermen van registraties
A.18.1.3	Beschermen van registraties	Procedure bewaartermijnen Johan
A.18.1.4	Privacy en bescherming van persoonsgegevens	JOHAN Portaal - Eigenaarschap van data, borging privacy en de AVG
A.18.1.4	Privacy en bescherming van persoonsgegevens	Meldingsformulier AP (Autoriteit Persoonsgegevens)
A.18.1.4	Privacy en bescherming van persoonsgegevens	Privacybeleid JOHAN
A.18.1.4	Privacy en bescherming van persoonsgegevens	Privacyverklaring JOHAN
A.18.1.4	Privacy en bescherming van persoonsgegevens	Verklaring beperking geografische opslag
A.18.1.4	Privacy en bescherming van persoonsgegevens	Verwerkingsregister JOHAN
A.18.2.1	Onafhankelijke beoordeling van IB	Auditplan Johan
A.18.2.2	Naleving van beveiligingsbeleid en normen	Directiebeoordeling IB Johan BV
A.18.2.3	Beoordeling van technische naleving	PEN Test Overeenkomst en vrijwaringsverklaring
A.19.1.1	Privacy officer	AP - aanmelding Functionaris Gegevensbescherming
A.19.1.1	Privacy officer	Meldingsformulier AP (Autoriteit Persoonsgegevens)
A.19.1.1	Privacy officer	Privacybeleid JOHAN
A.19.1.2	Privacybeleid	JOHAN Portaal - Eigenaarschap van data, borging privacy en de AVG
A.19.1.2	Privacybeleid	Privacybeleid JOHAN
A.19.1.3	Verwerkersovereenkomst	Hoofdovereenkomst Johan (Licentie/SLA/Verwerksovereenkomst)
A.19.1.3	Verwerkersovereenkomst	Verwerkersovereenkomst True Hosting
A.19.1.4	Melding datalekken	AP - aanmelding Functionaris Gegevensbescherming
A.19.1.4	Melding datalekken	Procedure Incident-probleem beheer en IC - Johan BV
A.19.1.5	Privacy impact assessment	DPIA Johan Portaal - 2021-04-02
A.19.1.6	Compliance	DPIA Johan Portaal - 2021-04-02
A.19.1.7	Privacy by design	JOHAN Portaal - Eigenaarschap van data, borging privacy en de AVG
A.19.1.8	Awareness	Ethische code Johan BV
A.19.1.8	Awareness	Informatiebeveiliging en privacy toets Johan

10 Bijlage: Johan Portaal

Informatiebeveiliging m.b.t. het Johan Portaal

Identificatie verwerkersketen / begripsdefinities m.b.t. het “Johan Portaal”

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.)

Het 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.

IB beleid m.b.t. het Johan Portaal

Met betrekking tot het Johan Portaal strekt de scope van IB beleid zich 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 verwerkersovereenkomsten 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.