BUREAU VOOR BEDRIJFSCOMMUNICATIE BV
Biesven 2, Postbus 99 5595 ZH Leende
Telefoon 040 2062933 Telefax 040 2062934

Informatiebeveiligingsbeleid

Beleidsafspraken m.b.t. de informatiebeveiliging

Innocom Bureau voor Bedrijfscommunicatie B.V.

CSI Service

Inhoudsopgave

1 Geldigheid en documentbeheer 3

1.1 Geldigheid document 3

1.2 Documentbeheer 3

2 Achtergrond 4

3 Eindverantwoordelijkheid 4

4 Doel, toepassingsgebied en gebruikers 4

5 Gerelateerde documenten 5

6 Basisterminologie 5

7 Beheersen van de informatiebeveiliging 6

7.1 Opzet informatiebeveiliging 6

7.2 Bedrijfscontinuïteit 7

7.3 Rolverdeling verantwoordelijkheden informatiebeveiliging 7

7.3.1 De directie 7

7.3.2 De Privacy Officer 8

7.3.3 De Security Officer 8

7.4 Communicatie Beleid 8

8 Beleidsuitgangspunten 9

1 Geldigheid en documentbeheer

1.1 Geldigheid document

Dit document is geldig vanaf 1-1-2020.

De eigenaar van dit document is de directie. Zij dient het document te controleren en het indien nodig minstens één keer per jaar bij te werken.

Wanneer de doeltreffendheid en toereikendheid van dit document worden beoordeeld, dan dienen de volgende criteria in ogenschouw te worden genomen:

- Het aantal geconstateerde beveiligingsincidenten
- Het aantal beveiligingsincidenten gerelateerd aan onvoldoende training van werknemers of bewustzijnsprogramma's voor wat betreft acceptabel gebruik van informatiebedrijfsmiddelen
- Het aantal werknemers en externe partijen die een rol hebben in de informatiebeveiliging, maar dit document niet kennen
- Niet-naleving van het informatiebeveiligingsbeleid met de wetten en regels, contractuele verplichtingen, en andere interne documenten van de organisatie
- Ineffectiviteit van de implementatie en het onderhoud van het informatiebeveiligingsbeleid
- Onduidelijke verantwoordelijkheden voor de implementatie van het informatiebeveiligingsbeleid

1.2 Documentbeheer

Documentgegevens	
Titel document	Informatiebeveiligingsbeleid
Onderwerp document	Beleidsafspraken m.b.t. de informatiebeveiliging
Versie	2.4
Status	definitief
Auteur	Pieter Philipsen
Documenteigenaar	Directie
Datum eerste concept	11-03-2019

2 Achtergrond

Het managementteam van Innocom Bureau voor Bedrijfscommunicatie B.V. (hierna: Innocom) onderkent dat het toenemende gebruik van datacommunicatiemogelijkheden (internet, E-commerce), de complexiteit van en verwevenheid tussen geautomatiseerde systemen, de massaliteit van de dagelijkse communicatie, de omvang van de bestanden alsmede de toenemende professionalisering van de computercriminaliteit leiden tot een grote afhankelijkheid en kwetsbaarheid van de geautomatiseerde informatievoorziening binnen Innocom.
De risico's die hiermee samenhangen zijn zeer aanzienlijk en kunnen een bedreiging vormen voor de vertrouwelijkheid, integriteit en continuïteit van de geautomatiseerde informatievoorziening en daarmee indirect voor het imago en dus de continuïteit van Innocom.

Daarnaast dwingt de privacywetgeving (GDPR-AVG) organisaties om de juiste verplichte maatregelen te treffen.

3 Eindverantwoordelijkheid

Gelet op de mogelijke impact van verstoringen op de continuïteit van Innocom berust eindverantwoordelijkheid voor het beleid inzake de beveiliging en de interne controle van de geautomatiseerde informatievoorziening bij de directie van Innocom. Dit wordt in de geldende privacywetgeving aangeduid als het accountabilityprincipe.

4 Doel, toepassingsgebied en gebruikers

Het doel van informatiebeveiliging is het beschermen van alle, in een organisatie aanwezige, (medische) gegevens & informatie tegen bedreigingen die de continuïteit van de organisatie in gevaar (kunnen) brengen. Een directe afgeleide daarvan is de bescherming van de privacy van de betrokkenen, t.w. eigen medewerkers, medewerkers van derde partijen en klanten.

Dit top-level beleid is gericht op het definiëren van het doel, de richting, de principes en de basisregels voor informatiebeveiliging.

Gebruikers van dit document zijn zowel alle werknemers van Innocom als die van relevante externe partijen.

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

5 Gerelateerde documenten

De aan dit document gerelateerde documenten zijn:

- Leeswijzer
- Het privacybeleid
- Het personeelshandboek, onderdeel informatiebeveiliging
- Het verwerkingsregister
- De incidentenprocedure / procedure Meldplicht Datalekken
- Registratie corrigerende maatregelen security incidenten
- De privacyverklaring

6 Basisterminologie

Informatiebeveiliging voorkomt of beperkt eventuele schade voor de organisatie. Afhankelijk van de vorm waarin informatie wordt gepresenteerd, dienen altijd passende beveiligingsmaatregelen te worden toegepast. Informatiebeveiliging zorgt dus voor het behouden van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie. Deze drie aspecten worden hieronder verder verklaart.

- Beschikbaarheid; de informatie moet op de gewenste momenten beschikbaar zijn voor de bevoegde gebruikers
- Integriteit; de informatie moet juist en volledig zijn en de informatiesystemen moeten juiste en volledige informatie opslaan en verwerken
- Vertrouwelijkheid; de informatie moet alleen toegankelijk zijn voor degene die hiervoor bevoegd is

Daarnaast zijn ook aspecten als authenticiteit en controleerbaarheid van belang.

- Authenticiteit betreft de mate van betrouwbaarheid van de originaliteit en herkomst van een document, een bericht, een gegeven of een ander object
- Controleerbaarheid heeft betrekking op de mate waarin de gegevens en de weergaven van de gegevens toetsbaar zijn.

Een ander belangrijk begrip binnen de informatiebeveiliging is het managementsysteem voor informatiebeveiliging. Dit managementsysteem is deel van het gehele managementproces dat zorgdraagt voor de planning, implementatie, het onderhoud, de beoordeling en het verbeteren van de informatiebeveiliging.

7 Beheersen van de informatiebeveiliging

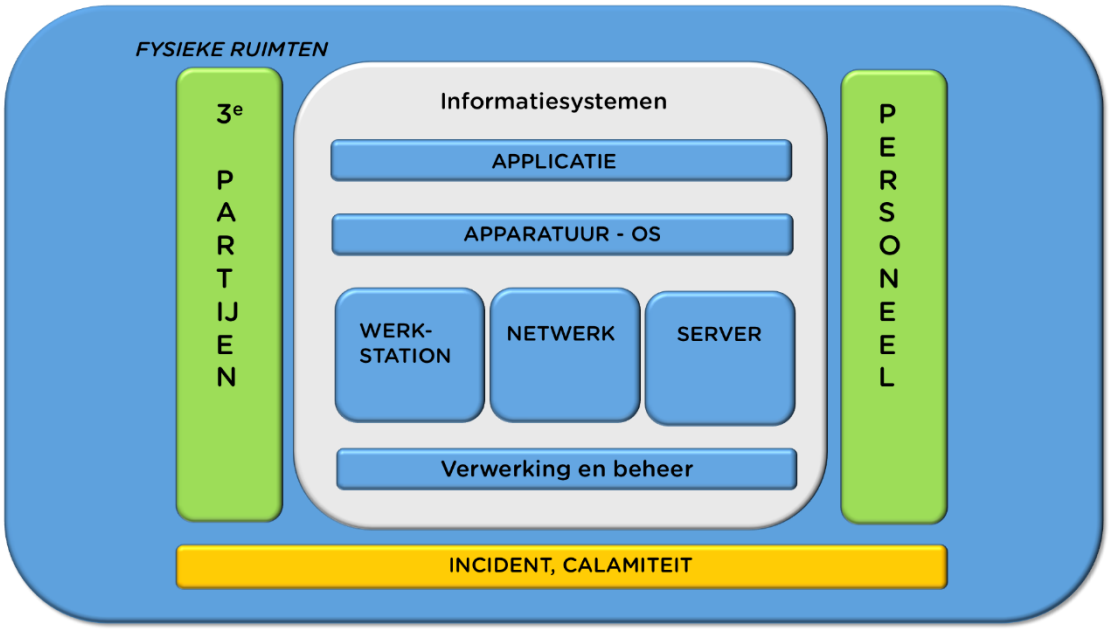
7.1 Opzet informatiebeveiliging

Van elk geautomatiseerd informatiesysteem, inclusief de daarbij behorende gegevens, dient expliciet één houder (verantwoordelijke) 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
- het (laten) ontwikkelen van adequate beveiligingsmiddelen
- interne controlemaatregelen.

Naast de applicatie betreft dit ook de juiste inzet van de infrastructurele componenten (werkstations, servers en LAN/WAN), 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.



Figuur 1: aandachtsgebieden informatiebeveiliging

Er wordt gesproken over eindverantwoordelijkheid omdat een aantal aspecten van het informatiesysteem uitbesteed wordt aan andere houders. Dit kan zowel betrekking hebben op aspecten tijdens de ontwikkeling of selectie van het systeem, als tijdens het beheer, het gebruik en/of bepaalde deelcomponenten van het totale systeem.

De te treffen maatregelen, alsmede de prioriteitsstelling hierin, dienen te worden bepaald op grond van een door het bedrijfsonderdeel periodiek op te stellen risicoanalyse, waarin:

- De bedreigingen tegen een betrouwbare en op continuïteit gerichte, geautomatiseerde informatievoorziening en de daarmee samenhangende risico's worden onderkend
- Een evenwichtig stelsel van onderling samenhangende maatregelen wordt ontwikkeld ter reducering van de risico's tegen acceptabele kosten.

Hierbij wordt derhalve niet een maximaal beveiligingsniveau nagestreefd, maar een optimaal niveau.

7.2 Bedrijfscontinuïteit

Bedrijfscontinuïteitsbeheer wordt beschreven in het calamiteitenbeheer.

7.3 Rolverdeling verantwoordelijkheden informatiebeveiliging

Buiten de in hoofdstuk 3 beschreven eindverantwoordelijkheid worden er binnen de informatiebeveiliging nog een aantal andere verantwoordelijke rollen onderkent. Deze rollen zijn: Privacy Officer en Security Officer. De verdeling van deze rollen is in de onderstaande tabel terug te vinden.

Rolverdeling verantwoordlijkheden informatiebeveiliging	
Privacy Officer	Krista van Hal
Security Officer	Pieter Philipsen

De onderstaande paragrafen geven een korte beschrijving van de taken van elke hierboven vermelde rol.

7.3.1 De directie

- De directie dient minstens één keer per jaar dit document te her beoordelen of elke keer wanneer zich significante wijzigingen voordoen.
- De directie stelt notulen op naar aanleiding van die vergadering. Het doel van de directieherbeoordeling is om de geschiktheid, toereikend en doeltreffendheid van het informatiebeveiligingsbeleid vast te stellen.
- De bescherming van de integriteit, beschikbaarheid en vertrouwelijkheid van bedrijfsmiddelen is de verantwoordelijkheid van de eigenaar van elke bedrijfsmiddel.
- Alle beveiligingsincidenten of zwakke punten moeten worden gemeld aan de Directie.

7.3.2 De Privacy Officer

- De Privacy Officer is verantwoordelijk voor het opstellen en onderhouden van o.a. het Privacy Beleid en het verwerkingsregister. Zij ziet toe op een zorgvuldige omgang met persoonsgegevens en controleert of de organisatie voldoet aan de privacywet en eventuele andere toepasselijke regelgeving.

7.3.3 De Security Officer

- De Security Officer is verantwoordelijk voor het onderhoud van het informatiebeveiligingsbeleid. Als zodanig houdt de Security Officer toezicht op de regels voor informatiebeveiliging en op de toepassing daarvan.
- De Security Officer is verantwoordelijk voor het, conform dit beleid, waarborgen van de implementatie en onderhoud van alle onderliggende procedures en werkinstructies en voor het waarborgen van de beschikbaarheid van de noodzakelijke middelen.
- De Security Officer zal bepalen welke aan informatiebeveiliging gerelateerde informatie zal worden gecommuniceerd naar derde partijen, zowel intern en extern, naar wie en wanneer.
- De Security Officer dient te waarborgen dat alle werknemers van Innocom, als ook alle van toepassing zijnde externe partijen die een rol hebben binnen de informatiebeveiliging, dit beleid kennen.

7.4 Communicatie Beleid

De Security Officer dient te waarborgen dat zowel alle werknemers van Innocom als ook alle van toepassing zijnde externe partijen die een rol hebben binnen de informatiebeveiliging, dit beleid kennen.

8 Beleidsuitgangspunten

T: Technisch

M: Mens

O: Organisatorisch

- T1: Logische toegangsbeveiliging zorgt ervoor, dat ongeautoriseerde personen of processen geen toegang krijgen tot de geautomatiseerde systemen, gegevensbestanden en programmatuur van Innocom.
- T2.1: Gebruikers van het informatiesysteem hebben alleen toegang tot die informatiebedrijfsmiddelen waarvoor uitdrukkelijk autorisatie aan hen is verleend door de eigenaar van het bedrijfsmiddel.
- T2.2: De gebruiker dient een andere persoon niet toe te staan, direct of indirect, gebruik te laten maken van zijn/haar toegangsrechten (d.w.z. gebruikersnaam, wachtwoord, enz.) en mag de gebruikersnaam en/of wachtwoord niet van een ander gebruiken.
- T2.3: De eigenaar van het gebruikersaccount is de gebruiker ervan. De gebruiker is verantwoordelijk voor het gebruik ervan en alle transacties uitgevoerd door dit gebruikersaccount.
- T2.4: Gebruikers dienen het geldende wachtwoordbeleid, zoals vastgelegd in het document Wachtwoordbeleid Innocom, te allen tijde op te volgen.
- T3.1: Gebruikers mogen het (medische) informatiesysteem alleen gebruiken voor de doeleinden waarvoor ze zijn geautoriseerd, d.w.z. voor welke ze rechten hebben gekregen.
- T3.2: Gebruikers van het informatiesysteem hebben alleen toegang tot die informatiebedrijfsmiddelen waarvoor uitdrukkelijk autorisatie aan hen is verleend door de eigenaar van het bedrijfsmiddel.
- T4.1: Werkplekken, met name werkplekken die het gebouw kunnen verlaten (notebooks, etc.), dienen te zijn encrypted (versleuteld) en dit moet gedocumenteerd worden door de ICT beheerder.
- T4.2: End-user computing is omgeven door zodanige maatregelen dat de vertrouwelijkheid en de integriteit van de opgeleverde informatie wordt gewaarborgd.
- T5: De fysieke en logistieke beveiliging van de datacentra en de bedrijfsgebouwen van Innocom is zodanig, dat de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens en gegevensverwerking gewaarborgd zijn.
- T6: Alleen bevoegd personeel is in staat het bedrijfspand zelfstandig te betreden. Gasten kunnen het gebouw alleen betreden onder begeleiding.
- T7: De bedrijf kritische apparatuur (servers, netwerkdevices, etc) dienen in een gecontroleerde ruimte opgeslagen te worden. Denk aan brandblusinstallaties, toegangscontrole, etc.
- T8.1: Teneinde computervirus of malware infecties te voorkomen wordt er slechts gewerkt met geautoriseerde versies van (legale) programmatuur.
- T8.2: Antivirussoftware dient op elke computer met automatische updates te worden geactiveerd.

- T8.3: Informatiesystemen dienen te worden voorzien van alle benodigde beveiligingsupdates.
- T9.1: Er dient een gedegen back-up procedure te worden opgesteld en nageleefd.
- T9.2: Het beheer en de opslag van gegevens zijn zodanig, dat geen informatie verloren kan gaan.
- T10: Er worden audit- en systeemlogbestanden bijgehouden waarin de activiteiten worden vastgelegd van de gebruikers.
- T12: De applicaties worden real-time van software-updates voorzien.
- T13: Er wordt gebruik gemaakt van Next Generation Firewalls inclusief een software-update abonnement.
- T14.1: Gegevensverstrekking intern en extern gebeurt op basis van 'need to know'. Medewerkers treffen maatregelen om te voorkomen dat informatie in handen van personen terechtkomt, die deze informatie niet strikt nodig hebben. Ook de toegang tot informatiesystemen wordt volgens dit principe adequaat beveiligd. Voor ICT-beheerders wordt hierop geen uitzondering gemaakt. Om te komen tot een betere service aan de gebruikers is het voor ICT-beheerders altijd mogelijk zich toegang te verschaffen.
- T14.2: Datatransport is zodanig met beveiligingsmaatregelen omkleed dat geen inbreuk kan worden gepleegd op de vertrouwelijkheid en de integriteit van de gegevens en op de informatievoorziening als geheel.
- T14.3: Opdrachten aan derden voor het uitvoeren van werkzaamheden worden zodanig omgeven met maatregelen dat er geen inbreuk op de vertrouwelijkheid, integriteit en continuïteit van de informatievoorziening kan ontstaan.
- T15: Bij de verwerking en het gebruik van gegevens worden maatregelen getroffen om de privacy van klanten en personeel te waarborgen.
- T16: Onderhoud op informatiesystemen en broncodes geschiedt binnen de kaders en regels van de vastgestelde ICT-architectuur volgens een standaardmethodiek, waarbij de documentatie volgens een vaste systematiek tot stand komt.
- T17: Aanschaf, installatie en onderhoud van geautomatiseerde gegevensverwerkende systemen, alsmede inpassing van nieuwe technologieën, en het gebruik van testdata, mogen geen afbreuk doen aan het niveau van veiligheid van de totale informatievoorziening.
- T18: Als er derde partijen zijn betrokken bij de verwerking van persoonsgegevens, dan zijn er de volgend maatregelen getroffen om dit conform de AVG-regels te verwerken: met alle 3^{e} partijen hebben we een verwerkingsovereenkomst afgesloten.
- T19: Bij de aanschaf van geautomatiseerde gegevensverwerkende systemen moet rekening worden gehouden met de principes "Privacy by Design" en "Privacy as Default" zoals deze zijn voorgeschreven in de Algemene Verordening Gegevensbescherming (AVG).
- T20: Gebruiker dient zich te houden aan het geldende beleid ten aanzien van het gebruik van internet, e-mail en uitwisseling van informatie met derde partijen zoals vastgelegd in het personeelshandboek.
- M1: Het personeelsbeleid is mede gericht op het leveren van een bijdrage aan de vertrouwelijkheid, integriteit en continuïteit van de informatievoorziening.
- M2: Elk bedrijfsmiddel (voor zover het geen flexplek-middelen zijn) heeft een aangewezen eigenaar in de Inventarisatie van Bedrijfsmiddelen. De eigenaar van het bedrijfsmiddel is verantwoordelijk voor de vertrouwelijkheid, integriteit en beschikbaarheid van informatie in het desbetreffende bedrijfsmiddel.

- M3, M4 en M5: Bij beëindiging van een arbeidscontract of een ander contract op basis waarvan diverse apparatuur, software of informatie in elektronische of papieren vorm wordt gebruikt, moet de gebruiker alle dergelijke informatiebedrijfsmiddelen retourneren aan zijn manager.
- O8: Er is een proces om incidenten adequaat af te handelen, te registreren en hier 'lessons learned' uit te trekken.
- O9: Er zijn calamiteitenplannen en -voorzieningen om de continuïteit van de bedrijfsvoering en de informatievoorziening te waarborgen en imagoschade te voorkomen.

Algemene uitgangspunten:

- Informatiebedrijfsmiddelen mogen alleen worden gebruikt voor bedrijfsbehoeften met als doel het uitvoeren van organisatie gerelateerde taken.
- Het is verboden om informatie te gebruiken op een manier die onnodige capaciteit vraagt, de prestaties van het informatiesysteem verzwakt of een bedreiging vormt voor de veiligheid.
- Apparatuur, informatie of software, ongeacht hun vorm of opslagmedium, mag niet van de locatie worden meegenomen zonder eerdere geschreven toestemming door afdelingsmanager.
- Clean desk-beleid: Indien de geautoriseerde persoon niet op zijn/haar werkplek definitie opnemen dat dit de pc/laptop betreft of toevoegen dat het ook thuis geldt zit, dienen zowel alle papieren, als ook gegevensopslagmedia gelabeld als gevoelig van het bureau of andere plaatsen (printers, faxmachines, kopieerapparaten, enz.) te worden verwijderd om ongeautoriseerde toegang te voorkomen. Dergelijke documenten en media dienen op een veilige manier te worden opgeslagen.
- Clear screen-beleid: Indien de geautoriseerde persoon niet op zijn/haar werkplek zit, dan dient alle gevoelige informatie op de computer te worden afgeschermd en dient de toegang via de schermen tot alle systemen waarvoor de persoon autorisatie heeft te worden geweigerd.
- In geval van een korte afwezigheid (tot 30 minuten), wordt het clear screen-beleid uitgevoerd door het scherm te vergrendelen met een wachtwoord of uit te loggen van alle systemen. Indien de persoon voor een langere periode afwezig is (meer dan 30 minuten), dan wordt het clear screen-beleid uitgevoerd door bij alle systemen uit te loggen en het werkstation uit te zetten.
- Documenten die gevoelige informatie bevat dienen direct van de printers, fax en kopieerapparaten te worden verwijderd.
- De fysieke en logistieke beveiliging van de datacentra en de bedrijfsgebouwen van Innocom is zodanig, dat de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens en gegevensverwerking gewaarborgd zijn.
- Het beheer en de opslag van gegevens zijn zodanig, dat geen informatie verloren kan gaan.
- Gebruikers mogen niet deelnemen aan activiteiten welke kunnen worden gebruikt om informatiebeveiligingsmaatregelen te omzeilen.
- Innocom heeft het recht de activiteiten van gebruikers en beheerders te loggen om problemen te kunnen oplossen, eventueel misbruik te kunnen detecteren en het gebruik van

de systemen te analyseren. De basis voor een succesvolle logging en monitoring bestaat uit een dusdanige vastlegging dat deze herleidbaar is tot het individu dat de gelogde activiteiten heeft uitgevoerd. Daarnaast dient ook de datum en tijd van de activiteit te worden gelogd. Hierbij dient er rekening te worden gehouden met synchronisatie van systeemklokken.

- Indien zich kritieke gebeurtenissen voordoen dient de technisch beheerder hiervan op de hoogte gesteld te worden. Tevens dient een beveiligingsincident te worden gemeld, waarna de procedure voor afhandeling van beveiligingsincidenten in werking treedt.