schuldenknooppunt

Beheersmaatregelen informatiebeveiliging

Schuldenknooppunt

Classificatie:	Vertrouwelijk
Auteur:	B. Tel (Axxemble)
Versie:	1.1
Datum:	24-09-2021

Inhoud

Inleiding

Dit document geeft invulling aan de beheersmaatregelen ten aanzien van informatiebeveiliging voor het Schuldenknooppunt. Onderscheid wordt gemaakt tussen de organisatie en de dienst (beide genaamd Schuldenknooppunt). Indien een beheersmaatregel specifiek van toepassing is op de dienst of de organisatie dan wordt dit aangegeven. In alle andere gevallen geldt de beheersmaatregel in brede zin.

Het document is opgezet aan de hand van de beheersmaatregelen zoals opgenomen in bijlage A van de ISO 27001:2020. Per onderdeel is aangegeven welke relatie het heeft met deze norm en eventuele andere normen.

De beheersmaatregelen in dit document zijn dienen geïnterpreteerd te worden als richtinggevend voor de invulling binnen operationele processen en systemen.

Beheersmaatregelen

De beheersmaatregelen zijn onderverdeeld naar de volgende onderwerpen:

- Informatiebeveiligingsbeleid
- Organiseren van informatiebeveiliging
- Veilig personeel
- Beheer van bedrijfsmiddelen
- Logische toegangsbeveiliging
- Cryptografie
- Fysieke beveiliging en beveiliging van de omgeving
- Beveiliging bedrijfsvoering
- Communicatiebeveiliging
- Acquisitie, ontwikkeling en onderhoud van informatiesystemen
- Leveranciersrelaties
- Beheer van informatiebeveiligingsincidenten
- Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
- Naleving

Informatiebeveiligingsbeleid

De organisatie heeft een beleidskader[1] opgesteld beleid t.a.v. informatiebeveiliging met goedkeuring van het bestuur.

Minimaal jaarlijks wordt het informatiebeveiligingsbeleid geëvalueerd aan de hand van een risicoanalyse om potentiële dreigingen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid te identificeren. Een wijziging in het risicoprofiel van de organisatie zal vertaald worden in aangepast beleid en bijbehorende maatregelen.

Bij significante wijzigingen binnen de organisatie of haar dienstverlening wordt het beleid eveneens herzien.

Het informatiebeveiligingsbeleid wordt - waar nodig - gecommuniceerd met relevante partijen waaronder medewerkers (ook inhuur), leveranciers en opdrachtgevers.

Normenkader	Referentie	Titel
ISO 27001	A.5.1.1	Beleidsregels voor informatiebeveiliging
ISO 27001	A.5.1.2	Beoordeling van het informatiebeveiligingsbeleid
NCSC	B.01	Informatiebeveiligingsbeleid
NCSC	B.03	Risicomanagement
SUWI	Artikel 6.4	Beveiliging elektronische voorzieningen SUWI

[1] Verwezen wordt naar Beleidskader informatiebeveiliging Schuldenknooppunt - v1.0.1 20-07-2021

Organiseren van informatiebeveiliging

Rollen en verantwoordelijkheden

De organisatie heeft de volgende rollen en verantwoordelijkheden vastgesteld t.a.v. informatiebeveiliging.

	Rol	Verantwoordelijkheden en bevoegdheden
	Directie	● Goedkeuring en vaststelling van het IB-beleid. ● Het vaststellen van de processen en de bepaling van het beveiligingsniveau. ● De totstandkoming van bewustzijn informatiebeveiliging en de risico´s. ● Het ter beschikking stellen van de middelen om de gestelde doelstellingen te kunnen realiseren. ● Het zorgdragen voor de evaluatie van de werking van het IB–beleid. ● Het zorgdragen dat de vastgestelde maatregelen in de praktijk kunnen en worden uitgevoerd, ● Ondersteuning van de medewerkers bij invoering van de maatregelen, ● Toezien op de correcte naleving van de maatregelen, ● Meewerken aan de uitvoering (en het oplossen) van audit (en bevindingen).
	Medewerkers	● Geheimhouding en zorgvuldigheid bij de uitvoering van activiteiten. ● De naleving van het IB-beleid en daarvan afgeleide processen, procedures, richtlijnen en het IB Management systeem; ● Rapporteren van incidenten en afwijkingen aan de security officer.
	Security officer	● Gedelegeerd eigenaar van het IB Management systeem. ● Strategische en tactische aansturing van het IB-managementproces. ● Functionele aansturing van medewerkers binnen het IB-managementsysteem. ● Opstellen en richting geven aan de IB aspecten in; ○ Beleidsvorming, ○ ICT-applicaties en organisatie, ○ Integrale risicobeheersing en compliance, ○ Bedrijfsprocessen, ○ Gebruikersorganisatie. ● Sturing geven aan en controle op; ○ Interne en externe assessments en audits, ○ Naleving in de gebruikersorganisatie, ○ Effectiviteit van geïmplementeerde IB maatregelen, ○ Correctieve en preventieve acties, ○ Afhandeling van klachten en incidenten. ● Ondersteunen van interne en externe assessments. ● Opvolging geven aan verbeteractiviteiten. ● Coördinatie bij IB-incidenten (inclusief klachten).

		● Incidentrapportages. ● Bewaking en onderhoud van geïmplementeerde maatregelen. ● Het assisteren bij de planning en uitvoering van interne en externe audits, ● Het monitoren en begeleiden van het oplossen van bevindingen n.a.v. de interne en/of externe audit.
	Interne auditor	● Controle op naleving van het IB-beleid binnen het aandachtsgebied, ● Ondersteunen van interne en externe assessments, ● Planning en uitvoering van interne audits, ● Het monitoren en begeleiden van het oplossen van bevindingen n.a.v. de interne audit.
	Functionaris Gegevensbescherming	● Toezicht op en advisering over naleving van de AVG en overige wet- en regelgeving m.b.t. de bescherming van persoonsgegevens.
	Privacy officer	● Coördinatie c.q. uitvoering van activiteiten in verband met naleving van de AVG en overige wet- en regelgeving m.b.t. de bescherming van persoonsgegevens.
	Office manager	● Coördinatie t.a.v. in- en uit dienst procedure alsook uitgifte en inname van bedrijfsmiddelen. ● Ondersteuning van de security officer (bij eventuele afwezigheid).
	Bestuur	● Bewaken en sturen op de realisatie van de doelstelling van de stichting in het algemeen en die van informatiebeveiliging in het bijzonder.
	Portefeuillehouder governance, privacy en security	● Namens het bestuur eindverantwoordelijk voor de informatiebeveiliging en de bescherming van persoonsgegevens.

De benodigde competenties voor het adequaat invullen van de verantwoordelijkheden worden getoetst en indien nodig aangebracht door middel van opleiding en training.

Projectbeheer

Met betrekking tot het uitvoeren van projecten wordt in de verschillende projectfasen aandacht en invulling gegeven aan:

- Initiatie
    - Vereiste rollen en verantwoordelijkheden binnen de projectorganisatie worden vastgelegd en toegepast.
    - De projectdocumentatie (en eventueel beheer van source code en overige configuratie items) wordt op gestructureerde wijze vastgelegd en toegang wordt op basis van genoemde rollen verstrekt.
    - Communicatie vindt binnen het project plaats op vertrouwelijke basis. Informatie wordt alleen gedeeld indien nodig en na toestemming van de verantwoordelijke(n). Indien nodig wordt een communicatieplan opgesteld.
- Uitvoering
    - Tijdens de uitvoering van het project wordt toegezien op naleving en toepassing van de beheersmaatregelen in dit document voor zover van toepassing.
    - Indien nodig (bijvoorbeeld bij wijzigingen) worden toegangsrechten aangepast na goedkeuring door de Office manager.
- Afsluiten
    - Na afronding van het project wordt de projectdocumentatie opgeruimd: overbodige informatie wordt verwijderd, andere informatie gearchiveerd.
    - Toegangsrechten / permissies worden ingetrokken. Toegang tot de gearchiveerde informatie is beschikbaar voor een beperkt aantal verantwoordelijken.

Normenkader	Referentie	Titel
ISO 27001	A.6.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging
ISO 27001	A.6.1.2	Scheiding van taken
ISO 27001	A.6.1.3	Contact met overheidsinstanties
ISO 27001	A.6.1.4	Contact met speciale belangengroepen
ISO 27001	A.6.1.5	Informatiebeveiliging in projectbeheer

Mobiele apparatuur en BYOD

De organisatie heeft geen eigen bedrijfsnetwerk en maakt uitsluitend gebruik van cloud services. Alle communicatie vindt daarom plaats via openbare of particuliere gastnetwerken, dit geldt ook voor mobiele apparatuur. Dit betreft met name laptops en smartphones, ook wanneer deze niet in eigendom zijn van de organisatie (BYOD).

Medewerkers zijn verantwoordelijk voor de beveiliging van mobiele apparatuur conform onderstaande richtlijnen:

- Toegang tot devices is afgeschermd met wachtwoord of pincode (patroon of swipe vergrendeling is niet toegestaan.
- Alle mobiele apparatuur dient gebruik te maken van encrypted opslag.
- Bij verlies van mobiele apparatuur wordt dit als incident geregistreerd en zal ook de procedure m.b.t. de meldplicht datalekken worden uitgevoerd.

Op basis van deze eisen is het toegestaan email van de organisatie te lezen op eigen smartphones.

De organisatie maakt geen gebruik van telewerk mogelijkheden (VPN etc.)..

Normenkader	Referentie	Titel
ISO 27001	A.6.2.1	Beleid voor mobiele apparatuur
ISO 27001	A.6.2.2	Telewerken

Veilig personeel

Screening

Wanneer de behoefte ontstaat voor een nieuwe medewerker n.a.v. vervanging, groei en/of verandering wordt op basis van de functieomschrijving een vacature opgesteld.

Kandidaten worden beoordeeld op basis van motivatie en CV en één of meer sollicitatiegesprekken. Referenties worden gevraagd en nagetrokken m.u.v. van ondersteunende functies.

Voor vertrouwensfuncties of functies die vanwege hun rol toegang tot gevoelige of vertrouwelijke informatie hebben (zoals bijvoorbeeld IT beheerders) dient een relevante Verklaring Omtrent Gedrag (VOG) aangevraagd te worden.

Identificatieplicht
De organisatie is verplicht identiteit van haar medewerkers te controleren. Voor aanvang van het dienstverband wordt het originele identiteitsbewijs gecontroleerd (dit kan bijvoorbeeld een paspoort zijn, een identiteitskaart of vreemdelingendocument). Een kopie hiervan wordt bewaard in het personeelsdossier.

Bij het controleren van identiteitsbewijzen wordt gelet op:

- De pasfoto: komt deze overeen met de persoon?
- Kenmerken: kloppen de genoemde fysieke kenmerken zoals lengte en leeftijd?
- Handtekening: aanwezig?
- Nationaliteit: is de nationaliteit vermeld? De identificatieplicht geldt ook voor buitenlandse werknemers.
- Geldigheid van het document, is de vervaldatum nog niet verstreken?

De kopie wordt bewaard zodat de organisatie bij eventuele controles, bijvoorbeeld door de Inspectie SZW, de gevraagde inlichtingen kan geven. De organisatie is verplicht de kopie te bewaren tot minimaal 5 jaar na het einde van het kalenderjaar waarin de werkzaamheden van de betreffende werknemer zijn beëindigd.

Medewerkers moeten zich te allen tijde kunnen legitimeren, ook tijdens het werk.

Arbeidsvoorwaarden

Het arbeidscontract en -reglement bevatten de wederzijdse verantwoordelijkheden ten aanzien van informatiebeveiliging.

Het arbeidscontract bevat afspraken ten aanzien van geheimhouding en naleving van het informatiebeveiligingsbeleid. De geheimhouding blijft ook van kracht na beëindiging van het dienstverband.

Alle informatie wordt bijgehouden in het personeelsdossier. Indien een VOG aangevraagd is wordt deze eveneens in het personeelsdossier opgenomen.

In dienst procedure

Alvorens een medewerker in dienst treedt dienen de volgende zaken gecontroleerd en verzameld te worden:

- Getekend arbeidscontract en -reglement ;
- Indien vereist voor de functie dient een VOG te worden aangevraagd ;
- Diploma's: een kopie van alle voor de functie relevante diploma's dient te worden overhandigd en te worden toegevoegd aan het personeelsdossier ;
- Kopie identiteitsbewijs ;
- Intakeformulier voor administratie voor het verwerken van salaris en pensioenopbouw (indien van toepassing).

Voor de indiensttreding worden de volgende zaken geregeld op technisch gebied:

- Activeren gebruikersaccount voor algemene diensten ;
- Activeren e-mailbox met voorletter.achternaam@organisatie.nl ;
- Uitgifte IT faciliteiten (bijvoorbeeld laptop / telefoon), medewerker tekent hierbij voor ontvangst alsook de bruikleenovereenkomst ;
- Uitgifte sleutel / toegangspas (plus eventueel alarm code) voor toegang tot kantoorfaciliteiten.

Voor alle zaken die in ontvangst genomen worden, wordt in tweevoud een ontvangstverklaring getekend.

De office manager draagt zorg voor de correcte uitvoering van de in dienst procedure.

Uit dienst procedure

Bij uitdiensttreding van een medewerker wordt op de laatste werkdag waarop de medewerker aanwezig is de onderstaande procedure uitgevoerd.

Bedrijfsmiddelen die bedrijfsinformatie bevatten dienen ingeleverd te worden op de laatste werkdag op kantoor.

De medewerker wordt gewezen op de van kracht blijvende geheimhouding die hij heeft getekend bij indiensttreding.

Verder dienen de volgende stappen ondernomen te worden:

- Toegang intrekken tot gebruikte diensten. Indien nodig wordt een reset gedaan van het wachtwoord (toegang) tot gedeelde accounts ;
- De-activeren e-mailbox. Indien gewenst kan e-mail tijdelijk doorgestuurd worden naar de office manager ;
- Inname van IT faciliteiten (bijvoorbeeld laptop / telefoon), medewerker tekent hierbij voor teruggave ;
- Inname van sleutel / toegangspas (plus eventueel intrekken / de-activeren alarm code) ;

Voor alle zaken die ingenomen worden, wordt in tweevoud een verklaring getekend.

Verder worden de administratieve zaken afgerond:

- Ontslagbrief tekenen ;

- Afmelden pensioenverzekeraar (indien van toepassing);
- Afmelden salarisadministratie.

De office manager draagt zorg voor uitvoering van de uit dienst procedure.

Bewustzijn

Medewerkers worden bij indiensttreding en minimaal één keer per jaar getraind ten aanzien van de risico's op het gebied van informatiebeveiliging.

Medewerkers dienen te allen tijde de gedragsregels te volgen.

Functiewijzigingen

Bij functiewijzigingen worden uitgegeven autorisaties allemaal ingetrokken en opnieuw uitgegeven conform de nieuwe functie.

Disciplinaire procedure

Wanneer medewerkers nalatig zijn, opzettelijke fouten en/of misbruik maken kan de medewerker hierop worden aangesproken. Hoewel medewerkers onderling elkaar kunnen aanspreken op elkaars gedrag, is het nemen van disciplinaire maatregelen voorbehouden aan de directie.

Overtreding

Het niet opvolgen van of houden aan het beleid en regels zoals die zijn vastgesteld worden beoordeeld als een 'overtreding' waarop deze procedure betrekking heeft.

De directie onderzoekt overtredingen, of het vermoeden daarvan, op vertrouwelijke wijze. Hierbij wordt getracht bewijzen te verzamelen die worden opgenomen in het personeelsdossier. Schorsing van een medewerker tijdens het onderzoek kan overwogen worden.

Procedure

Bij het vaststellen van een overtreding (zoals hierboven benoemd) kan de directie de volgende stappen nemen:

1. Informele waarschuwing / correctie;
2. Officiële waarschuwing;
3. Overplaatsing of wijziging van functie of demotie/degradatie;
4. Financiële boete (inhouding van (een deel van) het salaris);
5. Schorsing of op non-actief stellen;
6. Ontslag, eventueel op staande voet.

Hierbij geldt dat de verschillende stappen toegepast kunnen worden naar oordeel van de directie op basis van de zwaarte van de overtreding dan wel bij uitblijven van verbetering omtrent de overtreding. De stappen behoeven niet allen doorlopen te worden, de directie kan vrij besluiten welke maatregelen zij van toepassing acht. De directie streeft er naar medewerkers op een passende wijze te corrigeren en ziet ontslag als een uiterste maatregel die bij voorkeur voorkomen wordt.

Stappen 2 t/m 6 worden schriftelijk vastgelegd in het personeelsdossier en worden in een officieel gesprek aan de medewerker kenbaar gemaakt. Tijdens dit gesprek worden afspraken gemaakt over

verbetering van het gedrag t.a.v. de overtreding en de termijn waarop dit opnieuw geëvalueerd zal worden. Tijdens de evaluatie kunnen eventuele maatregelen teruggedraaid worden naar oordeel van de directie.

Bezwaar

Medewerkers hebben het recht bezwaar te maken tegen de verdenkingen en stappen zoals benoemd in deze procedure. Dit kunnen zij schriftelijk melden aan de directie of uiteindelijk bij de rechter. Bezwaar van de medewerker wordt eveneens vastgelegd in het personeelsdossier en de directie wordt geacht binnen één werkweek inhoudelijk hierop te reageren.

Normenkader	Referentie	Titel
ISO 27001	A.7.1.1	Screening
ISO 27001	A.7.1.2	Arbeidsvoorwaarden
ISO 27001	A.7.2.1	Directieverantwoordelijkheden
ISO 27001	A.7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
ISO 27001	A.7.2.3	Disciplinaire procedure
ISO 27001	A.7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband

Beheer van bedrijfsmiddelen

Bedrijfsmiddelen

De organisatie houdt een register van bedrijfsmiddelen bij. Per bedrijfsmiddel wordt de verantwoordelijke vastgelegd.

Bedrijfsmiddelen worden beschikbaar gemaakt via een uitgifte- en inname procedure. Bij uitgifte en inname wordt een ontvangstverklaring getekend.

Bij hardware middelen (bijvoorbeeld laptop / telefoon) wordt een bruikleenovereenkomst getekend waarin afspraken ten aanzien van aanvaardbaar gebruik zijn opgenomen.

Informatieclassificatie

Alle informatie, alsook alle betrokken systemen en applicaties, binnen de organisatie wordt geclassificeerd conform onderstaand classificatieschema.

Niveau	Beschikbaarheid	Integriteit	Vertrouwelijkheid
Geen	**Niet nodig** Gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn (bv: routeplanning)	**Niet zeker** Informatie mag worden veranderd (bv: templates en sjablonen)	**Openbaar** Informatie mag door iedereen worden ingezien (bv: algemene informatie op de website)
Normaal	**Belangrijk** Informatie mag korte tijd niet beschikbaar zijn (bv: administratieve gegevens)	**Beschermd** Het bedrijfsproces staat enkele (integriteits-) fouten toe (bv: rapportages)	**Intern** Informatie is toegankelijk voor alle medewerkers van de organisatie (bv: informatie op het intranet)
Hoog	**Noodzakelijk** Informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk (bv: primaire proces-informatie)	**Hoog** Het bedrijfsproces staat zeer weinig fouten toe (bv: bedrijfsvoerings-informatie en primaire proces informatie)	**Vertrouwelijk** Informatie is alleen toegankelijk voor een beperkte groep gebruikers (bv: persoonsgegevens, financiële gegevens)
Kritiek	**Essentieel** Informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten (bv: basisregistraties)	**Absoluut** Het bedrijfsproces staat geen fouten toe (bv: informatie uit het primaire proces)	**Geheim** Informatie is alleen toegankelijk voor direct geadresseerde(n)

			(bv: zorggegevens en strafrechtelijke informatie)

Documenten worden t.a.v. de vertrouwelijkheid gelabeld conform bovenstaande classificatie. Bij ontbrekende classificatie geldt de vertrouwelijkheid als *intern* tenzij dit uit de context kan worden opgemaakt (bijvoorbeeld marketing folders).

Informatie in e-mail en berichten wordt in principe als *vertrouwelijk* geclassificeerd en *intern* wanneer gericht aan groepen binnen de organisatie.

Indien de informatie *geheim* is, geldt dat dit expliciet aangegeven moet worden aan het begin van het bericht en nooit aan groepen mag worden verstuurd. Verder dient de communicatie in dit geval end-to-end versleuteld te zijn[2]. Voorbeeld voor aanduiding dat het bericht *geheim* is:

> *Let op: deze informatie is geheim.*

De geldende classificatie geldt voor zowel de tekst alsook de bijlagen. Tevens geldt dat de meest vertrouwelijke classificatie voor het geheel geldt.

Verwijderbare media

De organisatie staat het gebruik van verwijderbare media (bijvoorbeeld USB sticks) toe voor het tijdelijk bewaren / overzetten van openbare of interne informatie. *Vertrouwelijke* of *geheime* informatie mag niet worden opgeslagen op deze media.

Bij afschrijving of verwijdering van informatiedragende media (inclusief laptops, telefoons etc.) worden deze geschoond en vernietigd (secure erase / wipe).

Normenkader	Referentie	Titel
ISO 27001	A.8.1.1	Inventariseren van bedrijfsmiddelen
ISO 27001	A.8.1.2	Eigendom van bedrijfsmiddelen
ISO 27001	A.8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen
ISO 27001	A.8.1.4	Teruggeven van bedrijfsmiddelen
ISO 27001	A.8.2.1	Classificatie van informatie
ISO 27001	A.8.2.2	Informatie labelen

[2] Merk op dat voor email hier speciale maatregelen voor moeten worden genomen, berichtendiensten zoals Whatsapp zijn standaard end-to-end versleuteld.

ISO 27001	A.8.2.3	Behandelen van bedrijfsmiddelen
ISO 27001	A.8.3.1	Beheer van verwijderbare media
ISO 27001	A.8.3.2	Verwijderen van media
ISO 27001	A.8.3.3	Media fysiek overdragen
ISO 27001	A.11.2.4	Onderhoud van apparatuur
ISO 27001	A.11.2.5	Verwijderen van bedrijfsmiddelen
ISO 27001	A.11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein
ISO 27001	A.11.2.7	Veilig verwijderen of hergebruiken van apparatuur
ISO 27001	A.11.2.8	Onbeheerde gebruikersapparatuur
ISO 27001	A.11.2.9	‘Clear desk’- en ‘clear screen’-beleid
NCSC	B.06	ICT-landschap

Logische toegangsbeveiliging

Informatiesystemen en autorisaties

Per informatiesysteem is een verantwoordelijke systeemeigenaar vastgelegd. De systeemeigenaar is verantwoordelijk voor de beveiliging van het systeem conform het informatiebeveiligingsbeleid en voert indien nodig een risicoanalyse uit (of ondersteund hierbij).

Per informatiesysteem wordt door de systeemeigenaar vastgelegd welke rollen en permissies uitgegeven dienen te worden t.a.v. gebruikers van het informatiesysteem. Dit wordt vastgelegd in de autorisatiematrix.

Nieuwe gebruikers verkrijgen na goedkeuring van de office manager toegang tot de informatiesystemen conform de autorisatiematrix. Voor de eerste toegang dient een activatie-link of tijdelijk wachtwoord gebruikt te worden. Bij eerste toegang dient een nieuw wachtwoord ingesteld te worden.

Uitgegeven autorisaties worden minimaal jaarlijks beoordeeld (autorisatiecontroles). Voor kritieke systemen vindt dit minimaal eens per 3 maanden plaats.

Voor de dienst Schuldenknooppunt geldt verder een specifieke controle op aangesloten schuldhulpverleners vanwege het daaraan gekoppelde risico op misbruik en het lekken van persoonsgegevens.

Wachtwoorden

Voor toegang tot informatiesystemen gelden de volgende wachtwoordeisen:

- De minimale lengte is 12 karakters ;
- Een wachtwoord bevat minimaal één hoofdletter, één kleine letter, één cijfer en één speciaal teken ;
- Wachtwoorden mogen geen verwijzing bevatten naar de (gebruikers-)naam of e-mail;
- Een wachtwoord is maximaal 180 dagen geldig en dient hierna vernieuwd te worden ;
- Twee-factor autorisatie (2FA) wordt waar mogelijk toegepast. Bij gebruik van 2FA mogen wachtwoorden maximaal 365 dagen geldig blijven ;
- Opeenvolgende wachtwoorden (Welkom01, Welkom02 etc.) zijn niet toegestaan ;

Wachtwoorden dienen uitsluitend onthouden te worden door de betreffende personen. Het gebruik van een wachtwoordmanager wordt sterk aangeraden.

Groep-accounts zijn niet toegestaan.

Wachtwoorden mogen nooit in combinatie met de andere toegangsgegevens (gebruikersnaam, herstelopties etc.) gedeeld worden.

Indien mogelijk wordt toegang tot het informatiesysteem tijdelijk geblokkeerd na maximaal 5 inlogpogingen. Voor kritieke systemen is dit verplicht.

Informatiesystemen dienen wachtwoorden met sterke versleuteling (SHA-256+) en met gebruikmaking van een salt op te slaan.

Speciale toegangsrechten

Voor speciale toegangsrechten (bijvoorbeeld beheerdersrechten en voor toegang tot kritieke systemen) is 2FA en een maximale geldigheid van 180 dagen voor het wachtwoord vereist. De dienst Schuldenknooppunt wordt hierbij aangemerkt als kritiek systeem.

Er is voor alle informatiesystemen sprake van een scheiding tussen beheertaken en overige gebruikerstaken.

Beheerswerkzaamheden worden alleen uitgevoerd wanneer men is ingelogd als beheerder met een daarvoor gescheiden en persoonsgebonden account. Nadat de beheerstaken zijn uitgevoerd wordt weer teruggeschakeld naar een normaal gebruiksniveau.

Normenkader	Referentie	Titel
ISO 27001	A.9.1.1	Beleid voor toegangsbeveiliging
ISO 27001	A.9.1.2	Toegang tot netwerken en netwerkdiensten
ISO 27001	A.9.2.1	Registratie en afmelden van gebruikers
ISO 27001	A.9.2.2	Gebruikers toegang verlenen
ISO 27001	A.9.2.3	Beheren van speciale toegangsrechten
ISO 27001	A.9.2.4	Beheer van geheime authenticatieinformatie van gebruikers
ISO 27001	A.9.2.5	Beoordeling van toegangsrechten van gebruikers
ISO 27001	A.9.2.6	Toegangsrechten intrekken of aanpassen
ISO 27001	A.9.3.1	Geheime authenticatie-informatie gebruiken
ISO 27001	A.9.4.1	Beperking toegang tot informatie
ISO 27001	A.9.4.2	Beveiligde inlogprocedures
ISO 27001	A.9.4.3	Systeem voor wachtwoordbeheer
ISO 27001	A.9.4.4	Speciale systeemhulpmiddelen gebruiken
ISO 27001	A.9.4.5	Toegangsbeveiliging op programmabroncode
NCSC	B.02	Toegangsvoorzieningsbeleid
NCSC	U/TV.01	Toegangsvoorzieningsmiddelen

Cryptografie

Encryptie dient te worden toegepast op het transport van informatie indien het hoog/kritieke systemen betreft t.a.v. integriteit en/of vertrouwelijkheid.

Laptops en telefoons (mobiele apparatuur) dienen informatie versleuteld op te slaan, bij voorkeur volgens het pre-boot principe.

Informatiesystemen met kritieke vertrouwelijkheidseisen dienen de informatie encrypted op te slaan volgens het pre-boot principe. Encryptie vindt minimaal plaats op basis van AES 256 versleuteling of vergelijkbaar / sterker.

Encryptie-eisen

Voor verbinding en opslag gelden onderstaande eisen voor encryptie zoals gedefinieerd door NCSC. De organisatie hanteert hierbij het uitgangspunt dat het niveau 'Voldoende' volstaat voor alle toepassingen maar de voorkeur wordt gegeven aan 'Goed'.

De encryptie-eisen worden jaarlijks geëvalueerd.

Certificaten

De organisatie maakt uitsluitend gebruik van PKIOverheid certificaten.

Versies

De volgende TLS versies zijn toegestaan.

Niveau	Versie
Goed	TLS 1.3
Voldoende	TLS 1.2

Algoritmen

De veiligheid van een TLS-verbinding wordt gebaseerd op onderstaande algoritmes.

Niveau	Sleutel-uitwisseling	Certificaat-verificatie	Bulkversleuteling	Hashing
Goed / TLS 1.3	ECDHE	ECDSA / RSA	AES_256_GCM	SHA-384
Voldoende / TLS 1.2	(idem)	(idem)	(idem)	(idem)

Sleutellengtes

De veiligheid van RSA voor de versleuteling en digitale handtekeningen vereist onderstaande sleutellengtes.

Niveau	Sleutellengte	Elliptische kromme	Finite field-groep
Goed	3072 +	secp384r1 secp256r1 x448 x25519	ffdhe4096 (RFC 7919) ffdhe3072 (RFC 7919)
Voldoende	2048 - 3071 bit	(idem)	(idem)

Overig

- Compressie wordt bij voorkeur niet toegepast.
- OCSP stapling bij voorkeur wel.
- 0-RTT wordt bij voorkeur niet toegepast.
- Renegotiation wordt bij voorkeur niet toegepast.

Sleutelbeheer

Sleutelinformatie m.b.t. de encryptie worden volgens vaste procedures opgeslagen en gedurende de gehele levenscyclus beschermd.

Encryptie mag uitsluitend uitgevoerd worden door beheerders volgens de vastgestelde procedures.

Encryptiesleutels worden bewaard in een speciaal daartoe afgeschermde database.

Ten aanzien van de dienst Schuldenknooppunt zijn de maatregelen t.a.v. encryptie specifiek:

- Asymmetrische encryptie-sleutels worden opgeslagen in Azure Key Vault. Dit is een gespecialiseerde dienst voor het opslaan van encryptiesleutels.
- Berichten worden geëncrypt middels AES-256 encryptie. Er wordt voor ieder bericht een nieuwe sleutel gegenereerd. Verschillende berichten kunnen dus nooit één en dezelfde sleutel hebben.
- De AES Sleutel wordt ingepakt (versleuteld) m.b.v. een encryptiesleutel in Azure Key Vault. Er is hierbij geen directe toegang tot de sleutel. Het inpakken van de sleutel is alleen mogelijk door gebruik te maken van de Key Vault API.
- Het versleutelde bericht, kan vervolgens waar dan ook worden opgeslagen (in dit geval tijdelijk in de database en service-bus).

Normenkader	Referentie	Titel
ISO 27001	A.10.1.1	Beleid gebruik cryptografische beheersmaatregelen
ISO 27001	A.10.1.2	Sleutelbeheer
PKIoverheid		
NCSC	2021	ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)
NCSC	B.04	Cryptografiebeleid

Fysieke beveiliging en beveiliging van de omgeving

Voor kantoren, ruimten en faciliteiten is fysieke beveiliging ontworpen en deze wordt toegepast.

Toegangsmiddelen (sleutels / toegangspas / alarm code) worden via gecontroleerde uitgifte en inname beschikbaar gemaakt conform het beheer van bedrijfsmiddelen.

Ten behoeve van opslag van vertrouwelijke informatie vindt actief beheer van kasten en kluizen plaats.

Er vindt minimaal één keer per half jaar een controle/evaluatie plaats op de autorisaties voor fysieke toegang tot beveiligde zones.

Ten aanzien van de dienstverlening is de fysieke beveiliging, inclusief bescherming van nutsvoorzieningen uitbesteed aan ISO 27001 gecertificeerde hostingpartijen waarbij bescherming tegen onbevoegde toegang en schadelijke invloeden van buitenaf ingevuld zijn.

Normenkader	Referentie	Titel
ISO 27001	A.11.1.1	Fysieke beveiligingszone
ISO 27001	A.11.1.2	Fysieke toegangsbeveiliging
ISO 27001	A.11.1.3	Kantoren, ruimten en faciliteiten beveiligen
ISO 27001	A.11.1.4	Beschermen tegen bedreigingen van buitenaf
ISO 27001	A.11.1.5	Werken in beveiligde gebieden
ISO 27001	A.11.1.6	Laad- en loslocatie
ISO 27001	A.11.2.1	Plaatsing en bescherming van apparatuur
ISO 27001	A.11.2.2	Nutsvoorzieningen
ISO 27001	A.11.2.3	Beveiliging van bekabeling

Beveiliging bedrijfsvoering

Wijzigingsprocedure

Om de continuïteit van de dienstverlening en de veiligheid te garanderen worden wijzigingen op gecontroleerde wijze doorgevoerd.

- **Beleid**
  Beleidswijzigingen worden alleen met goedkeuring van het bestuur doorgevoerd. De goedkeuring wordt herkenbaar vastgelegd. Minimaal jaarlijks wordt het beleid door de directie geëvalueerd en beoordeeld en indien nodig aangepast en opnieuw vastgesteld.

- **Processen en procedures**
  Wijzigingen ten aanzien van processen en procedures worden gecontroleerd doorgevoerd na goedgekeurd te zijn door de directie.

- **Systemen**
  Wijzigingen met betrekking tot systemen worden doorgevoerd na goedkeuring van de systeemeigenaar en het succesvol afronden van tests en acceptatie. Voor kritieke systemen is de toepassing van het OTAP principe verplicht. Hierbij worden logisch gescheiden omgevingen gebruikt voor Ontwikkeling, Test, Acceptatie en Productie (OTAP).

- **Producten en diensten**
  Belangrijke wijzigingen t.a.v. de dienst Schuldenknooppunt worden altijd voorgelegd aan het bestuur ter goedkeuring.
  Alle wijzigingen in producten / diensten worden doorgevoerd via het ontwikkelproces. Deze ontwikkeling is feitelijk een proces van continue aanpassing/verbetering van producten en kent net als de systemen een test en acceptatiefase voordat wijzigingen in het definitieve / op te leveren product worden opgenomen.
  T.a.v. de dienst Schuldenknooppunt vinden major updates op productie uitsluitend plaats na het uitvoeren van een security assessment.

Malware

Op alle systemen van de gebruikers binnen de organisatie wordt een antivirus / antimalware scanner gebruikt voor de automatische detectie en blokkade van virussen, wormen, malware en spyware. Gebruikers kunnen dit niet uitschakelen.

Wanneer systemen voor een langere periode niet bijgewerkt worden of hebben gecommuniceerd met de server, zal hiervan een melding verschijnen dat er actie is vereist.

Back-up

De organisatie maakt uitsluitend gebruik van cloud diensten zoals geleverd door externe partijen / leveranciers. Back-up van informatie is onderdeel van deze dienstverlening en wordt vastgelegd in de overeenkomsten daartoe.

Opgemerkt wordt dat back-up m.b.t. de dienst Schuldenknooppunt van ondergeschikt belang is aangezien de uitgewisselde berichten tijdelijk en niet gegarandeerd aanwezig zijn. Verlies van deze berichten heeft daarmee een uiterst beperkte impact.

Restore tests

Gemaakte backups worden regelmatig (minimaal één keer per jaar per systeemtype) steekproefsgewijs gecontroleerd op de juiste werking van de backup- en restore-procedure en de mogelijkheid om de informatie daadwerkelijk te kunnen herstellen. Resultaat van de restore tests worden vastgelegd.

Monitoring en logging

Monitoring vindt plaats op beschikbaarheid, capaciteit en integriteit (foutmeldingen). Voor deze parameters worden per systeem / onderdeel de drempelwaarden bepaald waaraan moet worden voldaan. Wordt een dergelijke threshold overschreden dan wordt er een notificatie verstuurd aan de betreffende verantwoordelijke(n) / beheerders.

Alle notificaties worden vastgelegd en opgevolgd.

Logging

Bij het uitvoeren van monitoring is het loggen van informatie noodzakelijk. Dit omvat het beveiligen van de logs (bevoegdheid, beveiligen tegen inbraak of vervalsen, beschikbaarheid), kloksynchronisatie zodat deze overeenkomen met de juiste tijd (ook tussen logs van andere systemen) en het loggen van beheerders en de uitgevoerde beheertaken.

Logging wordt opgeslagen in systeembestanden die uitsluitend door de bron-applicaties kan worden geschreven. Gebruikers, inclusief administrators / beheerders, hebben geen directe schrijfrechten op de logbestanden.

Logbestanden worden met een roulatieschema van bij voorkeur 30 dagen bijgehouden (maximaal 12 weken). Na deze periode wordt de logging overschreven / verwijderd.

Logbestanden worden periodiek (bij voorkeur automatisch) gecontroleerd op onrechtmatige toegang of gebruik. Bij (het vermoeden van) incidenten dienen alle relevante logbestanden apart bewaard te worden om verlies van informatie / bewijs tegen te gaan.

Beheer van kwetsbaarheden

Systemen worden functioneel beperkt tot de functionaliteit en communicatiemogelijkheden die noodzakelijk is voor het correct functioneren van de dienstverlening (hardening), bij voorkeur op basis van een vaste configuratie baseline.

Alle geïnstalleerde software wordt via door de leverancier verstrekte updates actueel gehouden zodat eventuele kwetsbaarheden zo veel mogelijk voorkomen worden.

Voor desktop/laptops en smartphones worden updates waar mogelijk automatisch doorgevoerd.

Voor server systemen worden kritieke beveiligingsupdates zo spoedig mogelijk doorgevoerd. Overige updates van de software worden regelmatig geëvalueerd en na tests doorgevoerd tijdens gepland onderhoud.

Voor randapparatuur zoals firewalls, routers e.d. worden regelmatig firmware updates uitgevoerd wanneer hiermee beveiligingsproblemen opgelost worden.

Systeembeheerders houden zich via de media en specifieke trainingen op de hoogte van actuele bedreigingen ten aanzien van informatiesystemen.

Indien nog geen patch beschikbaar is dient gehandeld te worden volgens het advies van het Nationaal Cyber Security Centrum (NCSC).

Normenkader	Referentie	Titel
ISO 27001	A.12.1.1	Gedocumenteerde bedieningsprocedures
ISO 27001	A.12.1.2	Wijzigingsbeheer
ISO 27001	A.12.1.3	Capaciteitsbeheer
ISO 27001	A.12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen
ISO 27001	A.12.2.1	Beheersmaatregelen tegen malware
ISO 27001	A.12.3.1	Back-up van informatie
ISO 27001	A.12.4.1	Gebeurtenissen registreren
ISO 27001	A.12.4.2	Beschermen van informatie in logbestanden
ISO 27001	A.12.4.3	Logbestanden van beheerders en operators
ISO 27001	A.12.4.4	Kloksynchronisatie
ISO 27001	A.12.5.1	Software installeren op operationele systemen
ISO 27001	A.12.6.1	Beheer van technische kwetsbaarheden
ISO 27001	A.12.6.2	Beperkingen voor het installeren van software
ISO 27001	A.12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen
NCSC	U/WA.02	Webapplicatiebeheer
NCSC	U/PW.01	Operationeel beleid voor platformen en webservers
NCSC	U/PW.03	Webserver
NCSC	U/PW.05	Toegang tot beheermechanismen
NCSC	U/PW.07	Hardening van platformen
NCSC	U/PW.08	Platform- en webserverarchitectuur
NCSC	C.01	Servicemanagementbeleid
NCSC	C.06	Logging
NCSC	C.07	Monitoring
NCSC	C.08	Wijzigingenbeheer

NCSC	C.09	Patchmanagement
NCSC	C.10	Beschikbaarheidbeheer
NCSC	C.11	Configuratiebeheer

Communicatiebeveiliging

Post

Voor poststukken geldt dat vertrouwelijke informatie (hoog, kritiek) uitsluitend per aangetekende post verstuurd kan worden. Overige stukken mogen via de reguliere post verstuurd worden.

Email

Email wordt uitsluitend uitgewisseld met gebruik making van StartTLS (Start Transport Layer Security, directe encrypted communicatie op basis van TLS), DKIM (Domain Keys Identified Mail) en SPF (Sender Policy Framework).

Netwerkverkeer

Alle informatiesystemen met integriteits- en vertrouwelijkheidseisen dienen een beschermde vorm van communicatie te bieden conform het cryptografisch beleid.

Bij de communicatie gelden eisen op het gebied van encryptie, validatie en authenticiteit.

Niveau	Communicatiebeveiliging
Geen	-
Normaal	Gebruik van vaste protocollen en gebruikersauthenticatie
Hoog	Gebruik van vaste protocollen, gebruikersauthenticatie en encryptie van verkeer (vanuit beveiligde netwerkzone)
Kritiek	Gebruik van vaste protocollen, gebruikersauthenticatie, sterke encryptie van verkeer en validatie van berichten

De organisatie heeft geen eigen bedrijfsnetwerk en maakt uitsluitend gebruik van cloud services. Alle communicatie vindt daarom plaats via openbare of particuliere gastnetwerken.

Voor de dienst Schuldenknooppunt wordt de toegang gecontroleerd m.b.v. een firewall die op het 'block unless' principe is geconfigureerd. De firewall configuratie wordt minimaal elke 6 maanden gecontroleerd.

Beheersactiviteiten worden uitgevoerd vanuit een logisch gescheiden omgeving.

Normenkader	Referentie	Titel
ISO 27001	A.13.1.1	Beheersmaatregelen voor netwerken
ISO 27001	A.13.1.2	Beveiliging van netwerkdiensten
ISO 27001	A.13.1.3	Scheiding in netwerken

ISO 27001	A.13.2.1	Beleid en procedures voor informatietransport
ISO 27001	A.13.2.2	Overeenkomsten over informatietransport
ISO 27001	A.13.2.3	Elektronische berichten
ISO 27001	A.13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst
NCSC	U/PW.02	Webprotocollen
NCSC	U/PW.04	Isolatie van processen/bestanden
NCSC	U/PW.06	Platform-netwerkkoppeling
NCSC	U/NW.01	Operationeel beleid voor netwerken
NCSC	U/NW.02	Beschikbaarheid van netwerken
NCSC	U/NW.03	Netwerkzonering
NCSC	U/NW.04	Protectie- en detectiefunctie
NCSC	U/NW.05	Beheer- en productieomgeving
NCSC	U/NW.06	Hardening van netwerken
NCSC	U/NW.07	Netwerktoegang tot webapplicatie
NCSC	U/NW.08	Netwerkarchitectuur

Acquisitie, ontwikkeling en onderhoud van informatiesystemen

Eisen aan informatiesystemen

Bij de acquisitie en ontwikkeling van informatiesystemen worden beveiligingseisen als uitgangspunt genomen.

Relevant beveiligingseisen zijn in ieder geval (maar niet beperkt tot):

- Beveiligde toegang;
- Geautoriseerde (rolgebaseerde) toegang tot informatie;
- Beveiligde communicatie;
- Beveiligde opslag.

(Software-)ontwikkelproces

Met betrekking tot het ontwikkelen van met name software worden in de verschillende ontwikkelfasen aandacht en invulling gegeven aan:

- Ontwerpen
  - Beveiligingseisen vormen uitgangspunt voor nieuwe ontwerpen.
  - Het principe van privacy-by-design wordt toegepast waaronder het minimaliseren van de benodigde informatie, in het bijzonder persoonsgegevens.

- Realiseren
  - Source code wordt onder versiebeheer opgeslagen.
  - Toegang tot de source code is beperkt tot betrokken ontwikkelaars.
  - Bij het verwerken van informatie wordt de betrouwbaarheid van gegevens gewaarborgd door o.a. invoer- en uitvoervalidatie.
  - Gegevens worden enkel opgevraagd op basis van gecontroleerde queries.
  - Aanpassingen worden enkel doorgevoerd na een code review.

- Testen
  - Beveiligingseisen vormen het uitgangspunt voor het uitvoeren van (unit-)tests.

- Releasen
  - Uitsluitend na succesvol afronden van unit- en integratietests kan een nieuwe (software-)versie beschikbaar worden gemaakt voor acceptatie door de opdrachtgever(s).

De verschillende ontwikkelactiviteiten worden uitgevoerd in gescheiden omgevingen conform het OTAP principe.

Anonimisering van test data

Persoonsgegevens ten behoeve van het uitvoeren van test worden bij voorkeur gesimuleerd. Indien noodzakelijk ten behoeve van het testen of opsporen van problemen dienen persoonsgegevens geanonimiseerd te worden. Uitsluitend in de productieomgeving worden daadwerkelijke persoonsgegevens gebruikt en verwerkt.

Penetratietests

Kritieke systemen in eigen beheer, waaronder de dienst Schuldenknooppunt, worden na elke major release en minimaal jaarlijks getest middels een zogeheten penetratietest door een hiervoor erkende

partij. De penetratietest dient minimaal ‘grey box’ uitgevoerd te worden en in ieder geval te toetsen op de OWASP top 10.

Normenkader	Referentie	Titel
ISO 27001	A.14.1.1	Analyse en specificatie van informatiebeveiligingseisen
ISO 27001	A.14.1.2	Toepassingen op openbare netwerken beveiligen
ISO 27001	A.14.1.3	Transacties van toepassingen beschermen
ISO 27001	A.14.2.1	Beleid voor beveiligd ontwikkelen
ISO 27001	A.14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen
ISO 27001	A.14.2.3	Technische beoordeling van toepassingen na wijzigingen bedieningsplatform
ISO 27001	A.14.2.4	Beperkingen op wijzigingen aan softwarepakketten
ISO 27001	A.14.2.5	Principes voor engineering van beveiligde systemen
ISO 27001	A.14.2.6	Beveiligde ontwikkelomgeving
ISO 27001	A.14.2.7	Uitbestede softwareontwikkeling
ISO 27001	A.14.2.8	Testen van systeembeveiliging
ISO 27001	A.14.2.9	Systeemacceptatietests
ISO 27001	A.14.3.1	Bescherming van testgegevens
NCSC	U/WA.01	Operationeel beleid voor webapplicaties
NCSC	U/WA.03	Webapplicatie-invoer
NCSC	U/WA.04	Webapplicatie-uitvoer
NCSC	U/WA.05	Betrouwbaarheid van gegevens
NCSC	U/WA.06	Webapplicatie-informatie
NCSC	U/WA.07	Webapplicatie-integratie
NCSC	U/WA.08	Webapplicatiesessie
NCSC	U/WA.09	Webapplicatiearchitectuur
NCSC	C.03	Vulnerability-assessments
NCSC	C.04	Penetratietestproces

Leveranciersrelaties

Bij het aangaan van leveranciersrelaties met een belangrijke ICT component danwel verwerking van persoonsgegevens, moeten de volgende uitgangspunten in acht worden genomen.

De organisatie doet bij voorkeur alleen zaken met leveranciers die in het bezit zijn van een geldig ISO 27001 certificaat.

Met een leverancier moet een verwerkersovereenkomst (conform AVG artikel 28 lid 3) worden afgesloten indien er sprake is van "verwerking' (conform AVG artikel 4 lid 2) en de leverancier een verwerker is.

Indien mogelijk moet het "right-to-audit" worden opgenomen in leveranciersovereenkomsten. Voor leveranciers die als verwerker worden aangemerkt is dit verplicht. Voor leveranciers van kritieke diensten / systemen wordt minimaal jaarlijks een leveranciersbeoordeling uitgevoerd.

Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke toegang (fysiek, netwerk of informatie) de externe partij(en) moet(en) hebben en welke noodzakelijke beveiligingsmaatregelen hiervoor nodig zijn.

Informatiebeveiliging is aantoonbaar (op basis van een risicoafweging) meegewogen bij het besluit een externe partij wel of niet in te schakelen.

Beheersmaatregelen behorende bij risico's ten aanzien van leveranciersdiensten zijn voorafgaand aan het afsluiten van het contract gedefinieerd en geïmplementeerd.

In contracten met externe partijen is vastgelegd:

- hoe men om dient te gaan met wijzigingen en hoe ervoor gezorgd wordt dat de beveiliging niet wordt aangetast door de wijzigingen ;
- hoe wordt omgegaan met geheimhouding en de geheimhoudingsverklaring ;
- hoe escalaties en aansprakelijkheid geregeld zijn ;

Als er gebruikt gemaakt wordt van onderaannemers dan gelden daar dezelfde beveiligingseisen voor als voor de contractant. De hoofdaannemer is verantwoordelijk voor de borging bij de onderaannemer van de gemaakte afspraken.

Uitbestede ontwikkeling van programmatuur komt tot stand onder supervisie en verantwoordelijkheid van de uitbestedende organisatie. Er worden maatregelen getroffen om de kwaliteit en vertrouwelijkheid te borgen (bijv. stellen van veiligheidseisen, regelen van beschikbaarheid en eigendomsrecht van de code, certificatie, kwaliteitsaudits, testen en aansprakelijkheidsregelingen).

Normenkader	Referentie	Titel
ISO 27001	A.15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties
ISO 27001	A.15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten
ISO 27001	A.15.1.3	Toeleveringsketen van informatie- en communicatietechnologie
ISO 27001	A.15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers

ISO 27001	A.15.2.2	Beheer van veranderingen in dienstverlening van leveranciers
NCSC	B.05	Contractmanagement

Beheer van informatiebeveiligingsincidenten

Informatiebeveiligingsincidenten zijn als volgt gedefinieerd:

> Gebeurtenissen die kunnen leiden of hebben geleid tot *onbeschikbaarheid*, schending van *vertrouwelijkheid* en/of schending van *integriteit* van informatie die onder de verantwoordelijkheid van de organisatie valt.

Incidentenprocedure

Met betrekking tot het afhandelen van informatiebeveiligingsincidenten worden in de verschillende stappen aandacht en invulling gegeven aan:

- **Ontdekken en melden**
  - Alle (potentiële) informatiebeveiligingsincidenten dienen zo spoedig mogelijk te worden gemeld.
  - Alle informatiebeveiligingsincidenten worden geregistreerd.
- **Respons**
  - Er dient zoveel mogelijk relevant (bewijs-)materiaal te worden veilig gesteld voor analyse en onderbouwing.
  - (Tijdelijke) maatregelen (eventueel workaround) worden genomen om verdere schade van het informatiebeveiligingsincident zoveel mogelijk te voorkomen.
  - Op basis van alle beschikbare informatie wordt een oorzaak- en impactanalyse uitgevoerd.
  - Op basis van de analyse worden structurele maatregelen genomen om de oorzaak van informatiebeveiligingsincident weg te nemen en herhaling in de toekomst te voorkomen.
  - Alle relevante informatie met betrekking tot het informatiebeveiligingsincident wordt vastgelegd.
- **Lering en afsluiting**
  - Bij afsluiten van het informatiebeveiligingsincident wordt de uitvoering en uitkomst(en) van de incidentenprocedure geëvalueerd en indien nodig aangepast.

De security officer draagt zorg voor de uitvoering van de incidentenprocedure en communiceert met alle betrokken partijen.

Medewerkers verlenen medewerking aan het onderzoek en afhandeling van het informatiebeveiligingsincident.

Indien de impact van het informatiebeveiligingsincident groot is zal de security officer het incident escaleren naar de directie (bestuur). Eventueel kan hierbij het calamiteitenplan opgestart worden.

Datalek

Indien een informatiebeveiligingsincident een (potentieel) datalek betreft (in de zin van de AVG) treedt (ook) de procedure melden datalekken in werking.

De privacy officer draagt zorg voor de uitvoering van de procedure melden datalekken.

- De privacy officer beoordeelt (of laat beoordelen) of het informatiebeveiligingsincident ernstige nadelige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene(n) (datalek) en

besluit over het doen van de meldingen aan de Autoriteit Persoonsgegevens (AP) en aan de betrokkenen;
- De privacy officer doet de melding aan de AP en eventueel aan de betrokkene(n) (of laat dit doen);
- De privacy officer (ondersteund door de Functionaris Gegevensbescherming (FG)) is aanspreekpunt voor de AP en voorzien de AP voor zover noodzakelijk van nadere toelichting;
- Eventuele aanwijzingen van de AP worden vastgelegd en opgevolgd ;
- De privacy officer registreert het informatiebeveiligingsincident of vult deze aan met betrekking tot gegevens omtrent het datalek. Let op: onder de AVG moeten alle datalekken gedocumenteerd worden, ook datalekken die niet gemeld hoeven te worden aan de AP.

De FG is verantwoordelijk voor de advisering over de mogelijk gevolgen van een datalek voor de privacy van de betrokkene.

Normenkader	Referentie	Titel
ISO 27001	A.16.1.1	Verantwoordelijkheden en procedures
ISO 27001	A.16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen
ISO 27001	A.16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging
ISO 27001	A.16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen
ISO 27001	A.16.1.5	Respons op informatiebeveiligingsincidenten
ISO 27001	A.16.1.6	Lering uit informatiebeveiligingsincidenten
ISO 27001	A.16.1.7	Verzamelen van bewijsmateriaal

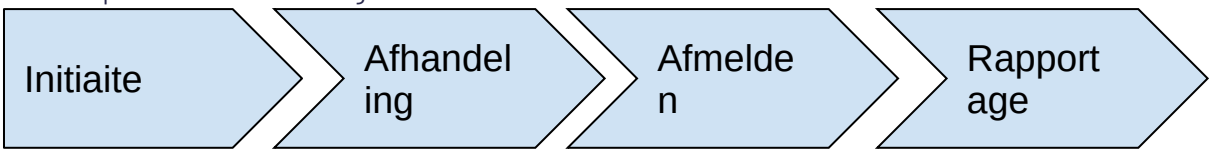
Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

Binnen de organisatie wordt jaarlijks de bedrijfscontinuïteit geëvalueerd door de directie waarbij de maatregelen t.a.v. de continuïteit herzien en/of uitgebreid worden.

De organisatie maakt geen gebruik van calamiteitsplannen t.a.v. specifieke calamiteiten maar past in deze gevallen een crisisprocedure toe. De crisisprocedure wordt minimaal jaarlijks beoordeeld en indien nodig herzien.

Crisisprocedure

De crisisprocedure kent de volgende fasen:



Initiatie

Voor de onderstaande mogelijke calamiteiten kan de crisisprocedure worden toegepast:

- Langdurige uitval van de dienstverlening (stroomuitval etc.) ;
- Substantieel verlies van informatie (crashes, diefstal, ransomware etc.) ;
- Escalatie van incidenten ;
- Wegvallen van sleutelpersonen ;
- Negatieve publiciteit.

Gebeurtenissen / calamiteiten of geëscaleerde incidenten die mogelijk volgens de crisisprocedure worden afgehandeld worden gemeld bij de office manager. De office manager bepaalt, eventueel in overleg met de security officer en andere relevante partijen, of er sprake is van een crisis waarvoor de crisisprocedure wordt toegepast.

Is dit het geval dan wordt de directie hiervan op de hoogte gesteld. De directie stelt vervolgens een crisismanager aan (bij beveiligingsincidenten veelal de security officer).

Afhandeling

Tijdens de afhandeling stuurt de crisismanager de organisatie aan om de crisis zo snel mogelijk op te lossen of terug te brengen tot beheersbare omstandigheden.

Overleg

Onder leiding van de crisismanager vindt er regelmatig overleg plaats tussen alle betrokken partijen. De directie kan hieraan deelnemen maar wordt hiervan in ieder geval geïnformeerd.

Communicatie

In onderstaand overzicht zijn enkele situaties die als calamiteit kunnen worden aangemerkt nader uitgewerkt inclusief een opzet voor de initiële communicatie richting deelnemers.

Situatie	Actie	Opmerkingen
Aanval op applicatie / datacenter	Toepassing van crisisprocedure. Getroffen deelnemers informeren.	Deelnemers informeren: *Er is op dit moment een verstoring van onze dienstverlening aan uw organisatie, dit komt door een aanval op onze infrastructuur. De aanval is gericht op de datacenter- leverancier waar wij apparatuur en data hebben staan die wij voor onszelf en voor deelnemers beheren. Wij willen benadrukken dat systemen en data niet in gevaar zijn, maar alleen de beschikbaarheid daarvan aantasten. Bij vragen kunt u contact opnemen met de Servicedesk.*
Uitval van verbinding / dienstverlening	Toepassing van crisisprocedure. Getroffen deelnemers informeren.	Deelnemers informeren: *Er is op dit moment een verstoring van onze dienstverlening aan uw organisatie. Onderzoek heeft uitgewezen dat dit veroorzaakt wordt door [… …]. Bij vragen kunt u contact opnemen met de Servicedesk.*
Wegvallen Project manager	Directie op de hoogte brengen. De office manager neemt taken en verantwoordelijkheden over.	Richting deelnemers communiceren m.b.t. veranderde situatie projectmanager.
Wegvallen Security Officer / Privacy Officer	Directie op de hoogte brengen. In overleg met directie wordt een nieuw persoon aangewezen die de taken eventueel over kan nemen. Indien nodig zal directie externe expertise inschakelen. De office manager neemt taken tijdelijke over.	

Afmelden

Wanneer, naar het oordeel van de crisismanager, de crisis verholpen is - opgelost dan wel tot een beheersbare situatie teruggebracht - wordt de crisis afgemeld en overgedragen aan de office manager.

Rapportage

De crisismanager maakt achteraf een rapportage op waarin de gang van zaken tijdens de crisis uiteen wordt gezet. De directie, crisismanager en office manager evalueren de afhandeling en communicatie en voeren indien nodig verbeteringen door in de crisisprocedure.

Verantwoordelijkheden

De volgende verantwoordelijkheden zijn tijdens de crisisprocedure van toepassing.

	Rol	Verantwoordelijkheden en bevoegdheden
	Directie	• Bepalen toepassing crisisprocedure en aanwijzen crisismanager. • Strategische aansturing en ondersteunen crisismanager. • Communicatie met publieke media (indien van toepassing.
	Crisismanager	• Tactische en operationele aansturing. • Autoriseren van (tijdelijke) preventieve / mitigerende maatregelen voor het voorkomen en terugdringen van schade als gevolg van de crisis. • Uitvoering van preventieve / mitigerende maatregelen. • Aansturing van medewerkers en toeleveranciers (indien van toepassing). • Communicatie met betrokken partijen, m.u.v. publieke media. • Crisisrapportage.
	Office manager	• Aanname potentiële crisissituatie en eventuele escalatie naar directie. • Overname bij afronding van de crisissituatie.
	Alle medewerkers (ook de rollen hier niet genoemd)	• Ondersteuning geven aan verzoeken tot uitvoering van preventieve en mitigerende maatregelen.

Redundantie

Kritieke systemen dienen met voldoende redundantie uitgevoerd te worden.

Normenkader	Referentie	Titel
ISO 27001	A.17.1.1	Informatiebeveiligingscontinuïteit plannen
ISO 27001	A.17.1.2	Informatiebeveiligingscontinuïteit implementeren
ISO 27001	A.17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren

ISO 27001	A.17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten

Naleving

Relevante wet- en regelgeving

De organisatie is gebonden aan de volgende wet- en regelgeving.

- AVG (en Uitvoeringswet AVG UAVG)
- Wet gemeentelijke schuldhulpverlening (Wgs)
- eHerkenning / Afsprakenstelsel Elektronische Toegangsdiensten
- Algemene Wet Rijksbelastingen, Artikel 52.4
- Telecommunicatiewet, Artikel 11.7a
- Auteurswet / intellectueel eigendom
- Wet computercriminaliteit

Het beleid en deze beheersmaatregelen geven invulling aan de informatiebeveiligings- aspecten van deze wet- en regelgeving.

Het delen van persoonsgegevens

De organisatie verstrekt geen persoonsgegevens aan derden.

Bewaartermijnen

Binnen de verschillende verwerkingen worden de bewaartermijnen gehanteerd zoals die binnen de wettelijke termijnen gehanteerd dienen te worden tenzij hier binnen de verwerking en met toestemming van betrokkenen een uitzondering op wordt gemaakt. Uitzonderingen kunnen alleen een verlenging inhouden, geen vermindering van de wettelijke bewaartermijn;

Voor (persoons-)gegevens waar geen wettelijke termijnen van toepassing zijn wordt de contractuele of binnen de verwerking vastgestelde termijn gehanteerd;

Het vernietigen van persoonsgegevens

Indien een betrokkene verwijdering van gegevens verlangt worden uitsluitend de niet-noodzakelijke gegevens verwijderd binnen de wettelijke bewaartermijn. Na verstrijken van de wettelijke bewaartermijn worden ook de overige gegevens verwijderd.

De organisatie zal persoonsgegevens vernietigen als ze niet meer nodig zijn voor het doel van de verwerking.

Rechten van betrokkenen

De organisatie geeft invulling aan het recht van betrokkenen ten aanzien van verwerkingen waarvoor het als verwerkingsverantwoordelijke geldt. Deze verzoeken omvatten:

- Inzage in opgeslagen (verwerkte) persoonsgegevens;
- Rectificatie en aanvulling van persoonsgegevens;
- Verwijdering (vergetelheid) van persoonsgegevens;
- Beperking van de verwerking;
- Bezwaar op de verwerking;
- Het recht op een menselijke blik bij geautomatiseerde besluitvorming en profilering;
- Overdraagbaarheid (dataportabiliteit) van persoonsgegevens;
- Het verkrijgen van duidelijke informatie (transparantie).

Voordat invulling gegeven wordt aan het recht wordt de betrokkene geïdentificeerd op basis van een controle van het identiteitsbewijs (paspoort, ID kaart of rijbewijs).

Audits en controles

De organisatie voert minimaal jaarlijks een controle uit op het informatiebeveiligingsbeleid en de (technische en organisatorische) beheersmaatregelen. Uitkomsten (bevindingen / afwijkingen) worden opgevolgd en vertaald naar een aangescherpte beveiliging.

Normenkader	Referentie	Titel
ISO 27001	A.18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen
ISO 27001	A.18.1.2	Intellectuele eigendomsrechten
ISO 27001	A.18.1.3	Beschermen van registraties
ISO 27001	A.18.1.4	Privacy en bescherming van persoonsgegevens
ISO 27001	A.18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen
ISO 27001	A.18.2.1	Onafhankelijke beoordeling van informatiebeveiliging
ISO 27001	A.18.2.2	Naleving van beveiligingsbeleid en -normen
ISO 27001	A.18.2.3	Beoordeling van technische naleving
NCSC	C.02	Compliancemanagement
NCSC	C.05	Technische controlefunctie

Bijlage: Lijst met afkortingen

Afkortingen en hun betekenis zoals gebruikt in dit document.

Afkorting	Betekenis
AES	Advanced Encryption Standard
(U)AVG	(Uitvoeringswet) Algemene Verordening Gegevensverwerking
AWR	Algemene Wet Rijksbelastingen
BIO	Baseline Informatiebeveiliging Overheid
DPIA	Data Protection Impact Assessment
EH3	eHerkenning niveau 3
FG	Functionaris Gegevensbescherming
IB	InformatieBeveiliging
ISO	International Standards Organisation (Internationale Organisatie voor Standaardisatie)
NCSC	Nationaal Cyber Security Centrum
NEN	NEderlandse Norm [3]
NVVK	Nederlandse Vereniging voor Volkskrediet
PKI	Public Key Infrastructure
PO	Privacy Officer
OTAP	(Gescheiden) Ontwikkel-, Test-, Acceptatie- en Productie- omgeving(en)
OWASP	Open Web Application Security Project
SLA	Service Level Agreement
(I)SO	(Information) Security Officer
SOC	Service Organization Control
Wgs	Wet Gemeentelijke Schuldhulpverlening

[3] NEN is tevens de naam van het samenwerkingsverband van de Stichting Koninklijk Nederlands Normalisatie Instituut en de Stichting Koninklijk Nederlands Elektrotechnisch Comité (NEC).

Bijlage: Gedragsregels

Alle medewerkers dienen onderstaande regels in acht te nemen met het doel de veiligheid de organisatie, haar deelnemers en de dienstverlening te waarborgen.

Het uitloggen op werkstation/laptop

- Bij het verlaten van de werkplek is het verplicht om het werkstation/laptop te vergrendelen.

Wachtwoorden

- Het opschrijven van wachtwoorden is niet toegestaan ;
- Het delen van wachtwoorden is niet toegestaan ;
- Let op dat niemand meekijkt bij het invoeren van een wachtwoord of mobiele code ;
- Een wachtwoord dient onmiddellijk gewijzigd te worden indien het vermoeden bestaat dat het bekend is geworden aan een derde.

Schriftelijke / verwijderbare informatie

- Het is uitsluitend toegestaan USB sticks te gebruiken voor het tijdelijk opslaan van openbare of interne informatie (dus geen vertrouwelijke of geheime informatie) ;
- Laat geen vertrouwelijke informatie op het bureau of werkplek liggen. Deze informatie dient altijd opgeborgen te worden in een afsluitbare opbergmogelijkheid (kast, locker) ;
- Verwijdering van vertrouwelijke documenten en/of welke persoonsgegevens bevatten dient plaats te vinden door middel van een papierversnipperaar.

Verlies of diefstal van apparatuur of papieren documenten

- Meld verlies of diefstal direct aan de security officer (of, indien niet aanwezig, de office manager;
- Maak een lijst op van gegevens (informatie) die verloren of gestolen zijn. Geef dit door aan de verantwoordelijke.

E-mail en social engineering

- Gebruik geen zakelijke e-mail voorzieningen voor privé e-mails ;
- Bij mail of telefonisch contact: stel de vraag waarom een verzoek wordt gedaan;
- Zet nooit gebruikersnaam en wachtwoord in een e-mail ;
- Controleer voor het versturen van elke e-mail of de juiste personen zijn toegevoegd voor wie de e-mail bestemd is en of de juiste bijlagen zijn toegevoegd ;
- Klik niet op een link indien daarom wordt verzocht in een ontvangen e-mail waarvan je de afzender niet kent of de boodschap (inhoud) onduidelijk is ;
- Stuur geen verdachte e-mails door. Bij wantrouwen: verifieer altijd de afzender, telefonisch of via andere kanalen.

Bijlage: Regels voor aanvaardbaar gebruik

Verboden activiteiten

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. Het is eveneens verboden om:

- Afbeeldingen of videobestanden te downloaden die geen bedrijfsdoel hebben, versturen van ketting e-mails, computerspelletjes te spelen, enz. ;
- Software op een lokale computer te installeren zonder expliciete toestemming van de leidinggevende;
- Java applicaties, Active-X controls en andere mobiele code te gebruiken, behalve wanneer door de security officer toestemming is verleend ;
- Cryptografische tools (encryptie) op de lokale computer te gebruiken, behalve ten behoeve van gevallen zoals gespecificeerd in de beheersmaatregelen informatiebeveiliging[4] ;
- Programmacodering van externe media te downloaden ;
- Randapparatuur te installeren of te gebruiken (zoals modems, memory cards of andere apparaten voor opslag en lezen gegevens, bijv. USB flash drives) zonder expliciete toestemming van de leidinggevende.

De organisatie kan een gespecialiseerde tool gebruiken met als doel het identificeren en blokkeren van verboden methoden van communicatie en het filteren van verboden inhoud.

Internetgebruik

De organisatie kan de toegang tot bepaalde internetpagina's voor individuele gebruikers, gebruikersgroepen of alle werknemers blokkeren. Indien de toegang tot sommige webpagina's is geblokkeerd, kan de gebruiker een geschreven verzoek indienen voor autorisatie voor toegang tot dergelijke pagina's. De gebruiker dient geen omweg te gebruiken. De gebruiker moet niet proberen om deze beperking zelfstandig te omzeilen.

De gebruiker is verantwoordelijk voor alle mogelijke gevolgen die voortkomen uit het onbevoegde of ongepast gebruik van internetdiensten of inhoud (content).

Back-up van laptop, desktop, etc.

De gebruiker dient alle bedrijfsinformatie opslaan op de daarvoor bestemde diensten van de organisatie. Een back-up is hiervan gegarandeerd.

Antivirus bescherming op bedrijfsmiddelen

De door de organisatie gebruikte antivirus software dient op elke computer met automatische updates te zijn geactiveerd.

---

[4] Verwezen wordt naar Beheersmaatregelen informatiebeveiliging Schuldenknooppunt - v1.1 24-09-2021

Verantwoordelijkheden gebruikersaccount

Het is een gebruiker verboden een andere persoon toe te staan, direct of indirect, gebruik te laten maken van zijn/haar toegangsrechten, d.w.z. gebruikersnaam, of te verlenen. Ook is het de gebruiker verboden de gebruikersnaam en/of wachtwoord van een ander te gebruiken.

Geheime authenticatie-informatie gebruiken

Bij het gebruik van wachtwoorden gelden de volgende regels:

- Wachtwoorden worden niet opgeschreven ;
- Gebruikers delen hun wachtwoord nooit met anderen. Groep-accounts zijn verboden ;
- Een wachtwoord moet onmiddellijk worden gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde ;
- Wachtwoorden mogen niet worden gebruikt in automatische inlogprocedures (bijv. opgeslagen onder een functietoets of in een macro).

Meenemen van bedrijfsmiddelen buiten de organisatie faciliteiten

Bestanden, apparatuur of software die het label *vertrouwelijk* dragen, of die bij openbaring aan derden het imago of de concurrentiepositie van de organisatie kunnen schaden, mogen zonder uitdrukkelijke toestemming van de directie niet buiten het kantoorgebouw te worden meegenomen (digitaal of op papier), of op systemen buiten het kantoorgebouw te worden geplaatst (door verzenden, opslaan, uploaden, etc.).

Onbeheerde gebruikersapparatuur

Gebruikers moeten:

- Actieve sessies beëindigen wanneer ze klaar zijn ;
- Zich afmelden, wanneer de sessie beëindigd is ;
- Onbeheerde mobiele apparatuur dient mee te worden genomen naar huis of opgeborgen in een afsluitbare kast ;
- Laptops, tablets en andere mobiele apparatuur beveiligen met behulp van een slot of vergelijkbare beveiliging (wachtwoord).