ConQuaestor
mastering finance

Raad voor Rechtsbijstand

Handboek

Informatiebeveiliging

Opdrachtgever
Raad voor Rechtsbijstand

Auteur
GV

Datum	Status	Versie
02-02-2011	Concept	v099

Inhoud

Voorwoord		5
1	Samenvatting	6
2	Inleiding	9
2.1	Achtergrond en context	9
2.2	Doelstelling	9
2.3	Kaderstelling	9
2.4	Scope	10
2.5	Op en aanmerkingen	12
2.6	Leeswijzer en versiebeheer	12
3	Structuur raamwerkinformatiebeveiliging	13
4	Informatiearchitectuur	15
5	Informatie Beveiligingsbeleid	17
5.1	Toelichting	17
5.2	Waarom informatiebeveiliging?	17
5.3	Wat zijn de bedreigingen voor de Raad?	17
5.4	Beleidsdocument voor informatiebeveiliging	17
5.5	Beoordeling van de informatiebeveiliging	19
6	Beheer van bedrijfsmiddelen	20
6.1	Verantwoordelijkheid voor bedrijfsmiddelen	20
6.2	Classificatie van informatie	21
7	Beheer van communicatie- en bedieningsprocessen	23
7.1	Bedieningsprocedures en verantwoordelijkheden	23
7.2	Beheer van de dienstverlening door een derde partij	23
7.3	Systeemplanning en –acceptatie	25
7.4	Bescherming tegen virussen en ‘mobile code’	26
7.5	Back-up	27
7.6	Beheer van netwerkbeveiliging	27
7.7	Behandeling van media	28
7.8	Uitwisseling van informatie	29
7.9	Controle	30
8	Toegangsbeveiliging	31
8.1	Bedrijfseisen ten aanzien van toegangsbeheersing	31
8.2	Registratie en beheer van gebruikers en hun toegangsrechten	31
8.3	Verantwoordelijkheden van gebruikers	32
8.4	Toegangsbeheersing voor netwerken	33
8.5	Toegangsbeveiliging voor besturingssystemen	33

8.6 Toegangsbeheersing voor toepassingen en informatie 34
8.7 Draagbare computers en telewerken 34

9 Verwerving, ontwikkeling en onderhoud van informatiesystemen 35
9.1 Beveiligingseisen voor informatiesystemen 35
9.2 Correcte verwerking in toepassingen 35
9.3 Beveiliging van systeembestanden 36
9.4 Beveiliging bij ontwikkelings- en ondersteuningsprocessen 37
9.5 Beheer van technische kwetsbaarheden 38

10 Beheersen van informatiebeveiligingsincidenten 39
10.1 Beheersing van informatiebeveiligingsgebeurtenissen en zwakke plekken 39

11 Beheerproces bedrijfscontinuïteit 40
11.1 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer 40

12 Naleving 41
12.1 Naleving van wettelijke voorschriften 41
12.2 Naleving van beveiligingsbeleid en -normen en technische naleving 41
12.3 Overwegingen bij audits van informatiesystemen 42

Bijlage I Richtlijnen voor classificatie conform de WBP 43

Bijlage II Nadere toelichting op de kaders voor de informatiebeveiliging van de Raad 46

Bijlage III Indeling van gegevensstromen naar beveiligingsniveau's 48

Voorwoord

De maatschappij wordt steeds informatie intensiever. Er worden steeds meer gegevens opgeslagen en deze gegevens hebben veel waarde. Zoals alles wat waarde heeft, dient dit goed beveiligd te worden. Dit geldt ook voor de Raad voor Rechtsbijstand. We leggen nu al een groot aantal gegevens gestructureerd vast in de database van GRAS en met de invoering van Filenet, gaan we ook de bijbehorende documenten digitaal vastleggen. De gegevens die we vast leggen zijn van dien aard dat mensen vertrouwen in onze organisatie moeten kunnen hebben dat wij hun zaak zo goed mogelijk en in vertrouwen behandelen. En op dit moment is dat ook zo.

Organisaties die het vertrouwen van hun klanten in het verleden geschaad hebben, hebben aanzienlijke financiële en reputatieschade opgelopen. Voor de Raad voor Rechtsbijstand zou dit kunnen leiden tot aanzienlijke reputatieschade. Dit betekent dat wij een verantwoordelijkheid hebben informatie zo goed mogelijk te beschermen. Dit is geen eenvoudige taak aangezien informatie ook zo efficiënt mogelijk beschikbaar dient te zijn voor alle betrokkenen, zowel onze klanten als onze medewerkers. Duidelijk is dat informatiebeveiliging niet een technisch probleem is. Bewustwording en organisatorische inrichting is minstens zo belangrijk. Om deze reden heeft de directie besloten om een beleidsdocument te schrijven die handvatten bevat voor iedereen binnen onze organisatie.

Samen met Toine Segers heb ik met veel plezier aan dit document gewerkt en ben er trots op om jullie hierbij de eerste versie van het integrale informatiebeveiligingsplan voor de Raad van Rechtsbijstand te mogen presenteren. Opmerkingen, wijzigingen en mogelijke verbeteringen hoor ik graag, zodat deze eventueel in een nieuwe versie kunnen worden verwerkt. Zo werken wij samen aan een steeds effectievere beveiliging van de informatievoorziening.

Tevens wil ik Giovanni Vierling en Joost Harskamp bedanken voor de ondersteuning bij het tot stand komen van dit plan.

Theo Mooren.
Hoofd Informatie Management

1 Samenvatting

De Raad voert een aantal maatschappelijke taken uit en is in grote mate afhankelijk van automatisering om deze taken uit te voeren. Bovendien verwerkt de Raad onder andere persoons- en zaakgegevens. Deze zijn privacy gevoelig, als deze gegevens onjuist zijn of als deze gegevens in de openbaarheid komen, kunnen klanten en relaties van de Raad hiervan aanzienlijke schade ondervinden. Het is daarom van belang dat de Raad als een goed huisvader met haar informatievoorziening om gaat.

Om de beveiliging van de informatievoorziening op gestructureerde wijze te borgen heeft de Raad op basis van de Code voor Informatiebeveiliging (NEN ISO27001/2) een raamwerk van informatie-beveiligingsmaatregelen getroffen. In de kern bestaat deze uit een beleid waarin het gewenste niveau van beveiliging is vastgelegd, een risicoanalyse en een beschrijving van passende maatregelen bij deze risico's. Om de complexiteit te beperken heeft de Raad ervoor gekozen om pragmatische aanpak te hanteren voor het uitvoeren van de risicoanalyse. Deze aanpak is erop gericht om per kwaliteitsaspect en per gegevensstroom een inschatting te maken van het gewenste beveiligingsniveau op basis van bedreigingen en de aard van de gegevens. De uitkomsten van deze analyse zijn in bijlage III van dit document vastgelegd.

Om het gewenste niveau van beveiliging aan te duiden, heeft de Raad een basisniveau voor informatie-beveiliging voor al haar systemen vastgesteld. Dit basisniveau bevat voldoende maatregelen om het merendeel van de bedreigingen het hoofd te bieden. Hiermee wordt een goede basis gelegd voor alle systemen. Voor die systemen, waarin extra gevoelige informatie wordt verwerkt of is opgeslagen, zijn aanvullende maatregelen geïdentificeerd en is ook een 'verhoogd' beveiligingsniveau vastgelegd.

In dit document zijn informatiebeveiligingsrichtlijnen beschreven voor bedrijfsmiddelen, communicatie en bedieningsprocessen, toegangsbeveiliging, verwerving en onderhoud van informatiesystemen, incidenten en bedrijfscontinuïteit. Onderstaande tabel geeft een samenvatting van deze richtlijnen gedifferentieerd naar de risico classificaties. Deze richtlijnen zijn in detail in de rest van dit document nader uitgewerkt.

De Raad heeft het beheer en het onderhoud van de applicaties en systemen uitbesteed aan Cap Gemini en Getronics. Dit informatiebeveiligingsbeleid is ook hierop van toepassing. De betreffende onderhouds- en beheercontracten zijn zodanig opgesteld dat aan de richtlijnen van dit document wordt voldaan.

Tabel 1 Samenvatting maatregelen informatiebeveiliging[1]

Samenvattig maatregelen gedifferentieerd naar risicoclassificatie		
	Basis	**Verhoogd**
Integriteit	Gebruikers krijgen uitsluitend rechten tot transacties in de applicaties op basis van hun functie. Deze rechten zijn vastgelegd in een autorisatiematrix. Aanvragen voor rechten worden aan deze matrix getoetst,	In applicaties en interfaces worden zowel detectieve als preventieve geautomatiseerde beveiligingsmaatregelen getroffen om de juiste, tijdige en volledige verwerking van gegevens te waarborgen.

[1] Bij verhoogd zijn uitsluitend de extra maatregelen genoemd.

	afwijkingen dienen door het daartoe bevoegde management te worden geaccordeerd. Controles in de diverse interfaces bewaken dat gegevens juist en volledig worden overgeheveld. Interfaces controleren de juistheid van de structuur en de volledigheid van de data voordat deze in een systeem wordt geladen. Wijzigingen in applicaties worden uitsluitend doorgevoerd nadat deze door het juiste niveau van management zijn goedgekeurd, goed zijn gedocumenteerd en goed getest. De Raad heeft procedures en werkinstructies opgesteld voor het gebruik en het beheer van bedrijfsmiddelen. Door netwerkbeveiliging en het gebruik van (sterke) authenticatie wordt voorkomen dat kwaadwillenden toegang hebben tot gegevens of muterende processen. Detectieve controles worden gebruik om de juistheid, tijdigheid en volledigheid van gegvensverwerkende processen te controleren.	Beheerders hebben uitsluitend toegang tot de productieomgeving na goedkeuring door IM. Deze toegang vindt uitsluitend plaats buiten de kantoortijden om. Toegang tot de systemen wordt door de beheerders vastgelegd in een log. Deze log wordt periodiek vergeleken met de automatische logging van de applicatie servers om vast te stellen dat geen ongeautoriseerde toegang heeft plaats gevonden.
Continuïteit	Dagelijks wordt een incrementele back-up gemaakt. Wekelijks wordt een full back-up gemaakt. Jaarlijks wordt het terugzetten van een back-up getest. De werking van deze procedure wordt jaarlijks gecontroleerd.	Maandelijks wordt de kwaliteit van de back-ups gecontroleerd 2maal per jaar wordt het terugzetten van een back-up gecontroleerd. De afgesproken SLA's waarborgen dat ingeval van een ernstig incident de dienstverlening binnen 24 uur wordt hersteld.

	De afgesproken SLA's waarborgen dat de dienstverlening binnen 48 uur wordt hersteld.	
Vertrouwelijkheid	Authenticatie op basis van complexe wachtwoorden Toegang op basis van een formeel aanvraag proces Gebruikers krijgen uitsluitend toegang tot die gegevens waartoe zij vanuit hun functie toegang toe moeten hebben. Dit is vastgelegd in een autorisatiematrix die wordt gehanteerd gebruikersbeheer. Netwerk beveiliging op basis van firewalls en sterke authenticatie voior systemen die toegang hebben vanaf een publiek netwerk. Beheerders hebben uitsluitend toegang middels sterke authenticatie. Alle toegang door beheerders wordt gelogd. Harde schijven van laptops zijn voorzien van encryptie.	Gegevens worden versleuteld opgeslagen op draagbare media Gegevens mogen niet per e-mail buiten de raad worden gecommuniceerd tenzij de e-mail of de inhoud is encrypted. Hard copy gegevens worden opgeruimd in een kast bij het verlaten van de werkplek. Het scherm van de gebruikte systemen wordt gelocked bij het verlaten van de werkplek. Interfaces en netwerkkoppelingen zijn encrypted.

2 Inleiding

2.1 Achtergrond en context

De Raad voor Rechtsbijstand (hierna: de Raad) heeft toezicht op en draagt zorg voor de organisatie van de verlening van gesubsidieerde rechtsbijstand door onder meer het Juridisch Loket (hierna: het JL), mediators en advocaten. Dit betekent dat rechtzoekenden met een relatief laag inkomen subsidie kunnen krijgen van de Raad. Vele duizenden huishoudens per jaar maken gebruik van gesubsidieerde rechtsbijstand.

Voor de toekenning van subsidies dient de advocaat of de mediator een verzoek in. De Raad voert vervolgens een aantal controles uit om vast te stellen of de rechtzoekende recht heeft op subsidie en keert vervolgens een inkomensafhankelijke subsidie uit aan de rechtsbijstandverlener. In dit proces wordt vertrouwelijke informatie van de rechtzoekende vastgelegd. Het gaat ondermeer om n.a.w. gegevens gekoppeld aan inkomensgegevens en algemene zaakgegevens. Om goed met deze vertrouwelijke informatie om te gaan heeft de Raad diverse beveiligingsmaatregelen getroffen.

Vanaf 1 februari 2009 zijn de vijf Raden voor Rechtsbijstand opgegaan in één Raad voor Rechtsbijstand. De nieuwe Raad heeft vestigingen in de hoofdsteden van de vijf ressorten van de gerechtshoven (Amsterdam, Den Haag, Arnhem, 's-Hertogenbosch en Leeuwarden). De ICT voorzieningen worden centraal aangestuurd vanuit de vestiging in Utrecht door de afdeling Informatie Management (hierna: de afdeling IM). Het is van belang dat informatiebeveiliging op ieder van de vestigingen op hetzelfde niveau is. Om dit te bewerkstelligen heeft de Raad één overkoepelend informatiebeveiligingsraamwerk opgesteld waarin de te treffen beveiligingsmaatregelen zijn vastgelegd. Dit document is het handboek informatiebeveiliging en bevat het informatiebeveiligingsbeleid en de informatiebeveiligingsrichtlijnen waaraan de Raad dient te voldoen. Het geeft een gedetailleerd beeld van de beveiliging van de informatieverwerking binnen de Raad.

2.2 Doelstelling

De doelstelling van dit document is om de organisatie van de Raad handvatten te bieden voor het oplossen van vraagstukken rondom informatiebeveiliging. Dit handboek beschrijft: het beleid, de uitgangspunten en richtlijnen betreffende de beveiliging van informatievoorziening bij de Raad.

2.3 Kaderstelling

De informatiebeveiliging van de Raad dient te voldoen aan de eisen van een aantal relevante wetten en regelgeving.

Wettelijk kader:

- Wet Bescherming Persoonsgegevens (WBP).

Ministerieel kader:

- Besluit Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR).

Overige kaderstelling:

- NEN-ISO/IEC 27002 Code voor informatiebeveiliging;
- Raamwerk Beveiliging Webapplicaties, uitgave van GovCert.

Deze wetten en richtlijnen zijn kaderstellend voor het informatiebeveiligingsbeleid van de Raad en zijn door de raad binnen het raamwerk informatiebeveiliging concreet vertaald in voor de Raad passende maatregelen.

In bijlage II is per kader een korte samenvatting gegeven van de inhoud en een kort (niet limitatief) overzicht van de belangrijkste eisen die van toepassing zijn.

2.4 Scope

In onderstaande paragrafen wordt nader toegelicht op welke processen en welke gebruikte technologie dit document van toepassing is. De Raad heeft ervoor gekozen om maatregelen in de organisatie, maatregelen met betrekking tot de wet schuldsanering natuurlijke personen en maatregelen met betrekking tot tolken en vertalers nog niet in dit document op te nemen. De strategische doelstellingen in dit document gelden echter ook voor deze activiteiten.

2.4.1 Processen

Dit document heeft betrekking op de informatie die verwerkt wordt in ondermeer de volgende processen:

- Reguliere toevoegingen;
- Lichte adviestoevoegingen;
- Mediation toevoegingen;
- Piket rooster;
- Behandeling bezwaar.

Een limitatieve lijst is opgenomen in bijlage IV.

2.4.2 Technologie

De informatieverwerkende processen van de Raad worden ondersteund door diverse applicaties. De volgende applicaties vallen binnen de scope van dit document:

- Gras;
- Workflow Management (WFM);
- Document Management (DM);
- De berichtenmakelaar (SoniqMQ);
- Interfaces (Star);
- TeamSoft;
- Rechtsbijstandverleners Informatie Systeem (RIS);
- Diverse websites (bijvoorbeeld: RvR.org, rechtwijzer.nl en www.rechtshulploket.nl);
- Generieke Correspondentie Systeem (GCS).

Ten behoeve van deze applicaties wordt door en voor de Raad infrastructuur beschikbaar gemaakt. De volgende infrastructuur componenten vallen binnen de reikwijdte van dit document:

- Windows server;
- Citrix;
- Netwerkcomponenten (routers en firewalls);
- WAN en LAN;
- DIGID koppeling;
- VPN verbinding (RSA token) voor thuiswerken.

De kwaliteit van gegevens uit diverse aanleverende systemen wordt als gegeven gezien. De Raad gaat er vanuit dat de gegevens uit de GBA en de belastingdienst als authentieke bronnen van zodanige kwaliteit zijn dat de Raad hierop geen zelfstandig onderzoek naar hoeft uit te voeren. (Conform de wet op de basis registraties.)

2.4.3 Code voor informatiebeveiliging

De Raad voor Rechtsbijstand hanteert de Code voor Informatiebeveiliging (NEN-ISO/IEC 27002) als basis voor het inrichten van een stelsel beveiligingsmaatregelen.

De Code voor Informatiebeveiliging bestaat uit de volgende onderwerpen:

a) Beveiligingsbeleid;
b) Organisatie van de informatiebeveiliging;
c) Beheer van bedrijfsmiddelen;
d) Personele beveiligingseisen;
e) Fysieke beveiliging en beveiliging van de omgeving (uitsluitend ICT);
f) Beheer van communicatie- en bedieningsprocessen;
g) Toegangsbeveiliging;
h) Aanschaf, ontwikkeling en onderhoud van informatiesystemen;
i) Beheersen van informatiebeveiligingsincidenten;
j) Beheerproces bedrijfscontinuïteit;
k) Naleving.

De Raad heeft ervoor gekozen om het organisatie deel van de code in eerste instantie nog niet in het raamwerkinformatiebeveiliging vast te leggen. Indien hier op een later tijdstip wel behoefte aan is, zal desbetreffend onderwerp worden opgenomen in dit beleidsdocument. Dit handboek is dan ook voornamelijk gericht op de technische beveiligingsmaatregelen ten aanzien van de volgende onderwerpen van de Code voor Informatiebeveiliging:

Tabel 2 Onderdelen van de ISO27002 in scope

Onderdeel Code	In dit handboek
Beveiligingsbeleid	Hoofdstuk 5
Beheer van bedrijfsmiddelen	Hoofdstuk 6
Beheer van communicatie- en bedieningsprocessen	Hoofdstuk 7
Toegangsbeveiliging	Hoofdstuk 8
Aanschaf, ontwikkeling en onderhoud van informatiesystemen	Hoofdstuk 9
Beheersen van informatiebeveiligingsincidenten	Hoofdstuk 10
Beheerproces bedrijfscontinuïteit	Hoofdstuk 11
Naleving	Hoofdstuk 12

2.5 Op- en aanmerkingen

Het handboek is een dynamisch document. Dit betekent onder meer dat de samenstellers zich aanbevolen houden voor elke vorm van commentaar. Voor inhoudelijke vragen, op- en aanmerkingen over het Handboek Informatiebeveiliging kunt u zich wenden tot:

Naam: Theo Mooren
Functie: Hoofd Informatie Management
Telefoon: 088 787 1070
Email: T.Mooren@rvr.org

2.6 Leeswijzer en versiebeheer

Hoofdstuk 1 van dit handboek informatiebeveiliging bevat een overzicht van de achtergronden van het informatiebeveiligingsbeleid en beschrijft de structuur van het raamwerk informatiebeveiliging. Hoofdstuk 2 bevat een samenvatting van het informatiebeveiligingsbeleid en legt een relatie naar de te treffen informatiebeveiligingsmaatregelen op tactisch niveau. Hoofdstuk 3 en verder beschrijven de getroffen beveiligingsmaatregelen per onderwerp in de code op tactisch niveau.

Doordat het Handboek Informatiebeveiliging een dynamisch document is, zullen periodiek nieuwe versie worden uitgegeven. In onderstaande tabel worden de wijzigingen ten opzichte van de vorige versie weergeven.

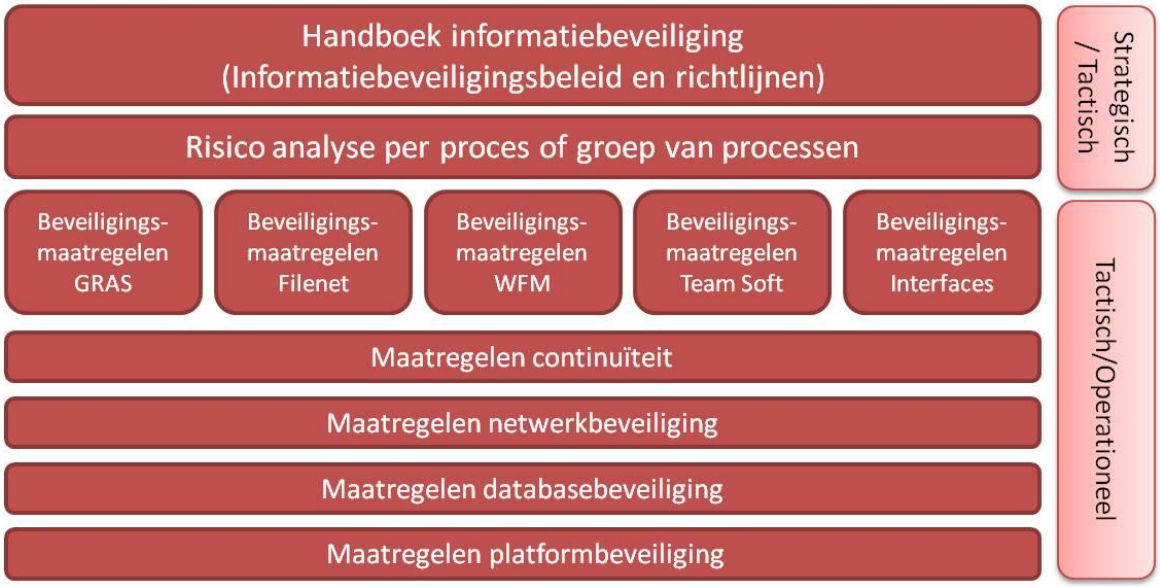
Versie	Uitgavedatum	Wijzigingen
V01	10 augustus 2010	Initiële opzet
V02 – V08	23 augustus 2010 – 17 november 2010	Aangevuld n.a.v. besprekingen met T. Mooren en T Segers.
V09	9 december 2010	Aangeboden en besproken in DRO
V099	5 januari 2011	Aangepast naar aanleiding van bespreking afvaardiging DRO en aangeboden aan DRO voor definitieve vaststelling

3 Structuur raamwerkinformatiebeveiliging

Het handboek informatiebeveiliging maakt onderdeel uit van een set van documenten die tezamen invulling geven aan de informatiebeveiliging van de Raad voor Rechtsbijstand: “het raamwerk-informatiebeveiliging”. Dit raamwerk bestaat uit:

1. het handboek informatiebeveiliging: hierin zijn op strategisch en tactisch niveau het informatiebeveiligingsbeleid, de doelstellingen en richtlijnen vastgelegd;
2. een risicoanalyse per proces of groep van processen: hierin worden mogelijke risico’s ten aanzien van de informatievoorziening vastgelegd en de mogelijke consequenties hiervan voor de Raad en haar klanten. Tevens bevat deze risicoanalyse een risicoclassificatie van de onderliggende systemen op basis waarvan informatiebeveiligingsmaatregelen dienen te worden getroffen;
3. een vastlegging van de informatiebeveiligingsmaatregelen: op operationeel niveau worden de richtlijnen geconcretiseerd in procedures, werkinstructies, handleidingen en andere concrete informatiebeveiligingsmaatregelen zoals het continuïteitsplan.

Schematisch kan dit raamwerk voor informatiebeveiliging als volgt worden weergegeven:



Informatiebeveiligingshandboek

In dit document wordt de structuur van het beveiligingsraamwerk beschreven en zijn tevens het informatiebeveiligingsbeleid en de informatiebeveiligingsrichtlijnen vastgelegd.

Informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid bevat op strategisch niveau de doelstellingen en uitgangspunten met betrekking tot informatiebeveiliging. Het informatiebeveiligingsbeleid fungeert als uitgangspunt bij het ontwerpen en implementeren van specifieke beveiligingsmaatregelen. Het informatiebeveiligingsbeleid wordt behandeld in hoofdstuk 2 en 3 van dit handboek.

Richtlijnen

In het informatiebeveiligingsbeleid wordt het gewenste beveiligingsniveau beschreven. Deze wordt op tactisch niveau nader uitgewerkt in richtlijnen waaraan de informatievoorziening van de Raad dient te voldoen om dit niveau te kunnen waarborgen. Een richtlijn is een schriftelijk vastgelegde aanwijzing voor een te volgen gedrag of handelwijze. De richtlijnen geven dus aan op welke manier wij ons binnen de

Raad moeten gedragen ten aanzien van de verwerking van vertrouwelijke informatie. Bijvoorbeeld, hoe vaak moeten wij ons wachtwoord wijzigen en welke regels gelden bij het samenstellen van een wachtwoord. Deze richtlijnen worden behandeld in hoofdstuk 4 en verder. De doelstelling van deze richtlijnen is richting te geven aan de ontwikkeling van nieuwe informatiesystemen, processen en procedures.

Risicoanalyse

In een risicoanalyse worden bedreigingen en impact met elkaar in verband gebracht. Het is gebruikelijk om een lijst met veel voorkomende bedreigingen te gebruiken om te analyseren welke impact deze bedreigingen, onafhankelijk van getroffen maatregelen, kunnen hebben op de bedrijfsvoering van de Raad. Op basis van de kans en de impact die op deze wijze worden geïdentificeerd, kunnen de risico's worden vastgesteld. Deze risico's worden geclassificeerd conform onderstaande figuur.

Kans / Impact	Beperkt	Middelgroot	Groot
Onwaarschijnlijk	Laag	Laag	Midden
Mogelijk	Laag	Midden	Hoog
Waarschijnlijk	Midden	Hoog	Hoog

Laag risico Het is onwaarschijnlijk dat de dreiging manifest wordt en de impact is beperkt. Beveiligingsmaatregelen van het basisniveau zijn afdoende om het risico tot een acceptabel minimum te beperken.

Midden risico Of wel het is onwaarschijnlijk dat de dreiging manifest wordt, echter de impact is groot of wel het is niet onwaarschijnlijk dat de dreiging manifest wordt echter de impact is naar verwachting beperkt. In beide gevallen is het basis beveiligingsniveau van de Raad voldoende om de risico's tot een acceptabel niveau te reduceren.

Hoog risico Zowel impact als de kans dat de dreiging manifest wordt is aanzienlijk. Er dienen preventieve maatregelen te worden getroffen en maatregelen dienen te worden getroffen om de impact te beperken.

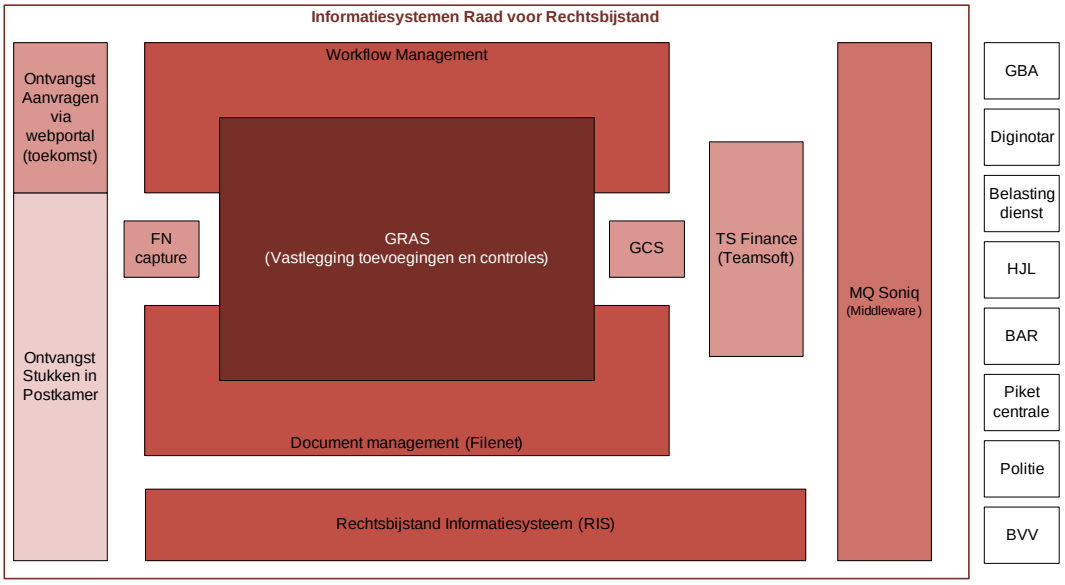
Beveiligingsmaatregelen

Op operationeel niveau zijn beveiligingsmaatregelen vastgelegd. Deze zijn vertaald in procedures werkinstructies, handleidingen en overige documenten. Het betreft een beschrijvingen van uit te voeren handelingen. Voorbeelden van handelingen zijn:

- het tekenen van een geheimhoudingsverklaring;
- het scannen van zaakgegevens;
- het aanvragen van autorisaties tot computersystemen en applicaties;
- het verlenen van toegang in verband met werkzaamheden;
- het uitvoeren van een periodieke controle door een verantwoordelijke manager.

4 Informatiearchitectuur

Onderstaande figuren bevatten een schematische weergave van de verschillende informatiesystemen van de Raad en hoe deze zich tot elkaar verhouden.



Ontvangststukken postkamer

In de postkamer worden fysieke poststukken ontvangen en gedistribueerd. Het betreft ondermeer fysieke aanvragen, zaakgegevens en diverse brieven. De stukken zijn vertrouwelijk en kunnen zeer vertrouwelijk zijn als het om concrete zaakgegevens of inkomensgegevens gaat. De fysieke stukken worden gescand en in filenet aan de juiste casus gekoppeld. De fysieke documenten worden vervolgens gearchiveerd. De medewerkers van de postkamer dienen deze stukken vertrouwelijk te behandelen. De stukken dienen na gebruik ofwel te worden vernietigd ofwel in een afgesloten ruimte te worden opgeslagen. Vanwege het belang van de stukken zijn procedures noodzakelijk om de volledigheid van de verwerking te waarborgen.

Ontvangst aanvragen via Webportaal (toekomst)

Verzoeken tot rechtsbijstand kunnen in de toekomst via het internet worden ingediend. In dat geval worden n.a.w gegevens en summiere gegevens betreffende de zaak middels een Web-formulier aan de back-office gezonden. Het betreft privacy gevoelige data. Het is dan ook van belang dat de afhandeling en verzending van het web-formulier aan een aantal strenge beveiligingseisen voldoet waaronder het schonen van de Cache en het versleuteld verzenden van de formulieren naar de back office. Voor deze applicatie geldt een verhoogd beveiligingsniveau.

FN Capture

Filenet Capture is de scan functie van filenet. Het wordt gebruikt om fysieke poststukken te scannen en aan een zaak te koppelen. Het is dan ook van belang om met goede procedures ervoor te zorgen dat alle documenten juist worden gescand zodanig dat deze aan de juiste zaak worden gekoppeld. Gezien het privacygevoelige karakter van de betreffende poststukken is het van belang om met procedures ervoor te zorgen dat de vertrouwelijkheid van deze gegevens is gewaarborgd. Voor dit systeem geldt een verhoogd beveiligingsniveau voor vertrouwelijkheid en integriteit.

Work Flow Management, GRAS en Document Management
De combinatie van Work Flow Management, GRAS en het Document Management systeem vormt het hart van de organisatie. Alle primaire processen en nagenoeg alle relevante informatie wordt door deze applicaties verwerkt en opgeslagen. De aard van de in deze applicaties opgeslagen data maakt dat deze aan het verhoogde beveiligingsniveau dienen te voldoen.

Generieke Communicatiesysteem (GCS)
Het GCS biedt de mogelijkheid om documenten die vanuit GRAS worden gegenereerd in Word te genereren en vervolgens aan te vullen. Dit systeem bevat geen vertrouwelijke informatie, maar is voor de werking van het primaire proces wel essentieel. Vandaar dat basis beveiligingsmaatregelen afdoende zijn, behalve voor het aspect continuïteit.

Webstar interface
De webstar interface verbindt het juridisch loket met GRAS en bevat Advocaat/mediator en kantoorgegevens en verwijsarrangementen. De informatie in deze interface is niet heel gevoelig. Beveiligingsmaatregelen zijn afdoende.

TeamSoft
De applicatie Open Finance van TeamSoft bevat privacy gevoelige gegevens, doordat de debiteuren en crediteuren gegevens in Team Soft zijn opgeslagen. Het is daarom van belang dat niet iedereen toegang heeft tot deze applicatie, te meer omdat ook betalingen vanuit Team Soft kunnen worden geïnitieerd. Gezien de aard van de applicatie en de organisatorische context is het basis niveau van beveiliging voor Team Soft voldoende.

MQ Soniq en externe interfaces
Vanuit GRAS worden gegevens gevalideerd met informatie uit externe bronnen zoals het GBA en de belastingdienst. Daarnaast worden ook gegevens aan de politie en het piketrooster gezonden. De gegevens die in de interface worden opgeslagen en verwerkt kunnen vertrouwelijk zijn. Bovendien is de beschikbaarheid van deze interface essentieel voor de dienstverlening door de Raad. De getroffen beveiligingsmaatregelen voor dit systeem zijn dan ook van het niveau verhoogd.

Rechtsbijstand Informatie Systeem (RIS)
Het RIS bevat Advocaat/mediator en kantoorgegevens en verwijsarrangementen. De data in deze applicatie is niet heel gevoelig. Ook is het systeem niet kritiek voor de primaire dienstverlening. Een Basis niveau is derhalve voldoende.

5 Informatie Beveiligingsbeleid

5.1 Toelichting

Informatiebeveiliging vormt een onlosmakelijk onderdeel van de dienstverlening van de Raad. Klanten van de Raad moeten erop kunnen vertrouwen dat de aan de Raad toevertrouwde informatie op een veilige manier wordt beheerd en verwerkt. Informatiebeveiliging omvat het geheel aan maatregelen dat dit vertrouwen beoogt te bewerkstelligen.

5.2 Waarom informatiebeveiliging?

Informatie en de systemen waarmee de informatie wordt verwerkt, zijn voor de Raad essentiële productiemiddelen. Net als voor veel bedrijven speelt de informatievoorziening voor de Raad een bepalende rol. Indien de informatievoorziening niet beschikbaar of niet betrouwbaar is, kan de dienstverlening van de Raad geen doorgang vinden. Binnen de processen van de Raad wordt vertrouwelijke informatie opgeslagen, indien deze informatie in de openbaarheid zou komen zou dit ernstige schade aan onze klanten kunnen toebrengen. Tevens zou dit ernstige imago schade voor de Raad opleveren.

De Raad beoogt een maatschappelijk verantwoordelijke bedrijfsvoering en dient daarom verantwoordelijk om te gaan met de informatie die zij verwerkt en opslaat namens haar klanten. Tevens willen we met dit beleidsdocument een aanzet geven om de continuïteit van onze bedrijfsvoering te waarborgen, door beleid en richtlijnen te definiëren over hoe wij onze data en informatiesystemen dienen te beveiligen.

5.3 Wat zijn de bedreigingen voor de Raad?

De informatievoorziening kan op verschillende wijzen worden bedreigd:

- fouten in hard- dan wel software;
- foutief menselijk handelen als gevolg van bijvoorbeeld foutieve instructies of verkeerde inschattingen;
- bewust foutief menselijk handelen, bijvoorbeeld fraude;
- storingen in technische faciliteiten zoals stroomstoringen;
- kwaadaardige software zoals computervirussen;
- illegale programmatuur;
- het gebruik van (onveilige) internet applicaties voor het delen van bestanden.

De mogelijke gevolgen hiervan zijn dat vertrouwelijke informatie bewust of onbewust wordt gedeeld met externe partijen zoals de pers, de politie of maatschappelijke groeperingen, dat de informatievoorziening voor een langere periode niet beschikbaar is of onjuiste informatie kan ervoor zorgen dat subsidies onterecht wel of onterecht niet worden uitgekeerd.

5.4 Beleidsdocument voor informatiebeveiliging

Doelstelling:

Informatiebeveiliging heeft tot doel de continuïteit, vertrouwelijkheid en integriteit van de informatievoorziening van de Raad te waarborgen door informatiebeveiligingsincidenten te voorkomen of de impact ervan te minimaliseren.

Informatiebeveiliging zorgt ervoor dat informatie kan worden uitgewisseld tussen systemen, afdelingen en organisaties en dat deze tegelijkertijd wordt beschermd. Het informatiebeveiligingsraamwerk richt zich op de volgende drie kwaliteitsaspecten:

- **integriteit**: de mate waarin de informatie juist, tijdig en volledig is;
- **continuïteit**: de mate waarin de informatievoorziening beschikbaar is en de mate waarin informatievoorziening ingeval van een calamiteit tijdig kan worden hersteld zonder dat hierbij onacceptabele informatie verliezen optreden;
- **vertrouwelijkheid**: de mate waarin de informatie uitsluitend door hiertoe bevoegden kan worden aangemaakt, geraadpleegd en gemuteerd.

Uitwerking:

De Raad heeft een raamwerk van informatiebeveiligingsmaatregelen vastgesteld. Dit raamwerk is gebaseerd op de code voor informatiebeveiliging. Om de complexiteit te reduceren onderscheidt de Raad twee niveaus van beveiliging: het basisniveau en een verhoogd niveau van beveiliging. De Raad heeft op basis van de Code een set van basis beveiligingsmaatregelen geïdentificeerd die voor alle informatiesystemen binnen de Raad gelden,het Basisniveau (overeenkomstig met risico classificatie I volgens definitie CBP). Een aantal systemen binnen de Raad bevat vertrouwelijke informatie, voor deze informatie geldt dat aanvullende maatregelen dienen te worden getroffen. Deze maatregelen zijn in het raamwerk aangeduid als Verhoogd beveiligingsniveau (overeenkomstig met risico classificatie II volgens definitie CBP).

Per gegevensstroom heeft de Raad een risicoanalyse uitgevoerd. In deze risicoanalyse is per kwaliteitsaspect (integriteit, continuïteit en vertrouwelijkheid) aangegeven in welke risicoklasse deze gegevensstroom valt. De maatregelen op basisniveau zijn zodanig gekozen dat deze voldoende zijn om de risico's voor risicoklasse laag en risicoklasse midden gegevensstromen tot een acceptabel minimum te reduceren. Alleen voor gegevensstromen met risicoklasse hoog worden verhoogde beveiligingsmaatregelen getroffen.

Richtlijnen:

Hieronder zijn de algemene richtlijnen ten aanzien van het informatiebeveiligingsbeleid opgenomen.

5.4.1 Het naleven van dit informatiebeveiligingsbeleid is verplicht voor de gehele organisatie van de Raad inclusief haar medewerkers, ingehuurden van derde partijen, dienstverleners en een ieder die toegang heeft tot de niet publieke informatie van De Raad.

5.4.2 Afwijkingen op onderdelen van dit beleidsdocument zijn toegestaan mits dit formeel is geautoriseerd door de directie en indien er dringende redenen zijn voor deze afwijking. Deze beslissing dient gedocumenteerd en opgeslagen te worden. Afwijkingen zonder geldige reden, of afwijkingen die niet juist zijn vastgelegd, zijn niet toegestaan. Het niet naleven van dit beleidsdocument wordt meegenomen in de beoordeling van medewerkers, ingehuurden van derde partijen en dienstverleners.

5.4.3 Iedere medewerker, inclusief ingehuurden van derde partijen, heeft de plicht om data en informatiesystemen te beschermen tegen ongeautoriseerde toegang, - gebruik, - aanpassingen, - openbaarmaking, - vernietiging of - overdracht en verlies.

5.4.4 De Raad zal actief informatiebeveiliging promoten binnen haar organisatie, waaronder haar medewerkers, ingehuurden van derde partijen en bezoekers.

5.4.5 De Raad hanteert procedures die het beheer van informatiebeveiliging meetbaar laat verlopen. De administratieve organisatie en interne controle is hierop aangepast.

5.4.6 De directie van de Raad zal er op toezien dat onderdelen van dit Informatie-beveiligingsbeleid vertaald worden in concrete beheersingsmaatregelen, toegespitst op de taken en verantwoordelijkheden van de betrokkenen.

5.4.7 Minimaal eens per 2 jaar zal de directie van de Raad het informatiebeveiligingsbeleid evalueren om vast te stellen of het nog steeds actueel is. Indien zich wijzigingen hebben voorgedaan in de informatievoorzieningsfunctie zullen de proceseigenaren een risicoanalyse uitvoeren om te bepalen of het nemen van additionele beheersingsmaatregelen noodzakelijk zijn.

5.4.8 Indien van toepassing zal het informatiebeveiligingsbeleid worden herzien en zal de hernieuwde versie beschikbaar gesteld worden aan alle belanghebbenden. Indien er een herziende versie van het informatiebeveiligingsbeleid wordt uitgegeven, zal de directie duidelijk communiceren aan de belanghebbenden dat een herziene versie van het informatiebeveiligingsbeleid beschikbaar is.

5.5 Beoordeling van de informatiebeveiliging

Doelstelling

Vast stellen dat de organisatie een geschikte, toereikende en doeltreffende aanpak van het beheer van informatiebeveiliging hanteert.

Richtlijnen:

5.5.1 Minimaal eens per jaar wordt een (onafhankelijke) beoordeling van de werking van het informatiebeveiligingsraamwerk geïnitieerd vanuit de directie. In de beoordeling worden de mogelijkheden voor verbetering en de noodzaak om wijzigingen aan te brengen in de beveiligingsaanpak, waaronder het beleid en de beheersdoelstellingen, meegenomen.

5.5.2 Een dergelijke beoordeling wordt uitgevoerd door personen die onafhankelijk zijn ten opzichte van de omgeving die wordt beoordeeld, bijvoorbeeld de controler, een onafhankelijke manager of een derde partij die in dergelijke beoordelingen is gespecialiseerd, voor zover zij beschikken over de juiste vaardigheden en ervaring.

5.5.3 De resultaten van de onafhankelijke beoordeling behoren te worden vastgelegd en aan de directie te worden gerapporteerd die de beoordeling heeft geïnitieerd. De verslagen behoren te worden bewaard.

6 Beheer van bedrijfsmiddelen

6.1 Verantwoordelijkheid voor bedrijfsmiddelen

Doelstelling:
Bereiken en handhaven van een adequate bescherming/beveiliging van bedrijfsmiddelen van de organisatie en waarborgen dat bedrijfsmiddelen het gewenste niveau van beveiliging krijgen.

Richtlijnen:

6.1.1 Alle bedrijfsmiddelen behoren te zijn verantwoord en aan een 'eigenaar' te zijn toegewezen.

6.1.2 De verantwoordelijke functionaris voor informatiebeveiliging beheert een overzicht van:

- programmatuur;
- gegevensbestanden;
- netwerkkoppelingen;
- documentatie;
- systeem- en proceseigenaren;
- de relaties tussen systemen, processen en informatie;
- de status van systemen (operationeel, in ontwikkeling);
- apparatuur;
- contracten van uitbestede diensten.

6.1.3 Voor alle bedrijfsmiddelen behoort een eigenaar bekend te zijn en er behoort te worden vastgelegd wie verantwoordelijk is voor het handhaven van geschikte beheersingsmaatregelen. De verantwoordelijkheid voor specifieke beheersingsmaatregelen mag door de eigenaar worden gedelegeerd, maar de eigenaar blijft verantwoordelijk voor een goede bescherming van de bedrijfsmiddelen. De eigenaren van systemen en data zijn verantwoordelijk voor:

- de juiste classificatie van het informatiesysteem;
- het toewijzen van autorisaties tot vertrouwelijke gegevens;
- periodieke evaluatie van de autorisaties;
- de toepassing van passende informatiebeveiligingsmaatregelen om de risico's te minimaliseren.

6.1.4 De beheerder van het overzicht van bedrijfsmiddelen wordt altijd op de hoogte gebracht van: aanschaf van bedrijfsmiddelen; installatie van bedrijfsmiddelen; verplaatsing van bedrijfsmiddelen en verwijdering van bedrijfsmiddelen.

6.1.5 Alle werknemers, ingehuurd personeel en externe gebruikers behoren zich te houden aan de regels voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die te maken hebben met IT-voorzieningen,waaronder:

a) regels voor elektronische post (e-mail) en gebruik van internet;
b) richtlijnen voor het gebruik van draagbare apparatuur, in het bijzonder voor gebruik buiten het terrein van de organisatie.

6.2 Classificatie van informatie

Doelstelling:

Het belang van de kwaliteitsaspecten (continuïteit, integriteit en vertrouwelijkheid) dient voor de individuele bedrijfsmiddelen en informatiesystemen te worden geëvalueerd. Hierop gebaseerd worden deze bedrijfsmiddelen geclassificeerd voor elk van de kwaliteitsaspecten, zie bijlage III.

Het doel van deze classificatie is om het gewenste beveiligingsniveau voor ieder bedrijfsmiddel vast te stellen. De classificatie vindt plaats op basis van een risicoanalyse.

Richtlijnen:

6.2.1 Effectieve beveiligingsniveaus kunnen per bedrijfsmiddel of informatiesysteem verschillen. Om het juiste niveau van beveiliging vast te stellen, dient de eigenaar het bedrijfsmiddel of het informatiesysteem op basis van een risicoanalyse aan te geven in welke risicoklasse het informatiesysteem of bedrijfsmiddel moet worden geclassificeerd.

6.2.2 Overeenkomsten met externe partijen waarin het delen van informatie aan de orde is behoren procedures te omvatten voor de identificatie van de classificatie van die informatie en voor het interpreteren van de classificatielabels van andere organisaties. Tevens dienen deze contracten afspraken te bevatten over te treffen beveiligingsmaatregelen in relatie tot de classificatie van de uitgewisselde gegevens.

6.2.3 De Raad heeft gekozen voor een baseline benadering. Dit houdt in dat voor alle informatie in ieder geval een basisniveau van beveiliging is ingericht. Deze baseline is vastgelegd in dit beleidsdocument. Voor gegevens met een hoog risico voor integriteit, vertrouwelijkheid en continuïteit dienen aanvullende maatregelen te worden getroffen, deze maatregelen zijn vastgelegd met de classificatie beveiligingsniveau “verhoogd”.

In onderstaande tabellen wordt de definitie van de beide beveiligingsniveaus vastgelegd.

Integriteit		
	Definitie	**Voorbeeld**
Basis	Gegevens waarvoor geldt dat onjuistheid of onvolledigheid beperkte schade voor de Raad, advocatuur of de klant kan betekenen.	Document templates Advocaat/mediator – en kantoorgegevens Interne telefoonlijst
Verhoogd	Gegevens waarvoor geldt dat onjuistheid of onvolledigheid grote schade voor de Raad, advocatuur of de klant kan betekenen.	Inkomensgegevens zaaksgegevens Declaraties

Continuïteit		
	Definitie	**Voorbeeld**
Basis	Gegevens waarvoor geldt dat indien de dienstverlening niet tijdig kan worden hersteld, slechts beperkte schade voor de Raad, advocatuur of de klant kan ontstaan.	Debiteurengegevens Crediteurengegevens Financiële informatie Declaraties

Continuïteit		
Verhoogd	Gegevens waarvoor geldt dat indien de dienstverlening niet tijdig kan worden hersteld, grote schade voor de Raad, advocatuur of de klant kan ontstaan.	Webportaal, aanvragen

Vertrouwelijkheid		
	Definitie	**Voorbeeld**
Basis	Gegevens waarvoor geldt dat ongewenste openbaarmaking of verspreiding beperkte schade voor de Raad, advocatuur of de klant kan betekenen.	N.A.W. gegevens Declaratiegegevens Interne telefoonlijst
Verhoogd	Gegevens waarvoor geldt dat ongewenste openbaarmaking of verspreiding grote schade voor de Raad, advocatuur of de klant kan betekenen.	Gegevens over strafzaken Inkomensgegevens

In bijlage III is per gegevensstroom voor ieder relevant kwaliteitsaspect het gewenste beveiligingsniveau weergegeven.

7 Beheer van communicatie- en bedienings-processen

7.1 Bedieningsprocedures en verantwoordelijkheden

Doelstelling:

Waarborgen van een correcte en veilige bediening van IT-voorzieningen. Er behoren verantwoordelijkheden en procedures te worden vastgesteld voor beheer en bediening van alle IT-voorzieningen. Dit omvat tevens de ontwikkeling van geschikte bedieningsinstructies.

Er behoort waar van toepassing, functiescheiding te worden toegepast om het risico van nalatigheid of opzettelijk misbruik van systemen te verminderen.

Richtlijnen:

7.1.1 De bedieningsprocedures behoren de instructies te geven voor een gedetailleerde uitvoering van elke taak,waaronder:

a) verwerking en behandeling van informatie;
b) back-ups;
c) eisen ten aanzien van de planning, waaronder onderlinge verbondenheid met andere systemen, start van de eerste taak en beëindiging van de laatste taak;
d) instructies voor de afhandeling van fouten en andere uitzonderlijke situaties die zich tijdens de uitvoering van de taak kunnen voordoen, waaronder beperkingen in het gebruik van systeemhulpmiddelen;
e) contactpersonen voor onverwachte bedieningsmoeilijkheden of technische storingen;
f) instructies voor de behandeling van bijzondere uitvoer en media, zoals het gebruik van speciaal papier of het beheer van vertrouwelijke uitvoer, waaronder procedures voor een veilige verwijdering van uitvoer van mislukte taken;
g) procedures voor het opnieuw opstarten en herstellen van het systeem in geval van systeemstoringen;
h) beheer van ‘audit trail’ en systeemlogbestand-informatie.

7.1.2 Bedieningsprocedures en de gedocumenteerde procedures voor systeemactiviteiten behoren als formele documenten te worden behandeld en wijzigingen behoren te worden geautoriseerd door de directie.

7.2 Beheer van de dienstverlening door een derde partij

Doelstelling:

Waarborgen van een geschikt niveau van informatiebeveiliging en dienstverlening in overeenstemming met de overeenkomsten voor dienstverlening door een derde partij. De Raad controleert de implementatie en de naleving van de overeenkomsten om te waarborgen dat de geleverde diensten aan alle eisen voldoen die met de derde partij zijn overeengekomen.

Richtlijnen:

7.2.1 De afspraken die de Raad maakt met derde partijen inzake gegevensverwerking dienen te worden vastgelegd in zogenoemde “Service Level Agreements” (SLA). Deze SLA’s dienen, indien van toepassing, te beschrijven:

a. de functionaliteit van de diensten:

i. de aangeboden functies;
ii. de openstellingtijden;
iii. eventuele gebruikersondersteuning en opleidingen;

b. de prestatie-eisen die aan de dienst gesteld worden:
i. beschikbaarheid;
ii. response tijden;
iii. probleemherstel en onderhoudsronden;
iv. informatiebeveiliging;
v. calamiteitenregeling;

c. de restricties die gelden, bijvoorbeeld:
i. maximaal aantal (gelijktijdige) gebruikers;
ii. maximaal aantal transacties;

d. een beschrijving van de relevante administratieve aspecten:
i. de geldigheidsduur van de SLA;
ii. de regeling die gehanteerd wordt voor verlenging van de geldigheidsduur;
iii. de regeling die gehanteerd wordt voor wijziging van de SLA;
iv. de systematiek die gebruikt wordt voor het bepalen van de kosten, en de wijze waarop de kosten in rekening gebracht worden;
v. de regeling die gehanteerd wordt voor de afhandeling van geschillen en het omschrijven van een eventuele derde partij die daarbij een rol kan spelen;
vi. de aansprakelijkheid van beide partijen;
vii. een beschrijving van omstandigheden waarin beroep op overmacht gedaan kan worden;
viii. het aangeven van de rapportages die verplicht zijn en welke frequentie daarvoor geldt;
ix. werkoverleg dat geïmplementeerd wordt en wie daarvan deel uitmaakt;
x. een geheimhoudingsclausule;
xi. een boeteclausule.

7.2.2 De beveiligingseisen die in de SLA's worden afgesproken dienen minimaal de eisen uit dit handboek te omvatten.

7.2.3 De securityofficer dient te waarborgen dat de volgende aspecten van de dienstverlening door een derde partij nageleefd wordt:

a) de prestatieniveaus van de dienstverlening dient minimaal eens per jaar te worden getoetst, door een onafhankelijke partij, om te bepalen of deze in overeenstemming zijn met de overeenkomsten;
b) de dienstverleningsrapporten opgesteld door de derde partij dienen te worden beoordeeld en, voor zover nodig volgens de overeenkomsten, dienen er ten minste vier keer per jaar voortgangsvergaderingen te worden georganiseerd;
c) de leverancier van de dienstverlening dient informatie te verstrekken over informatiebeveiligingsincidenten, de bijhorende beoordelingen en hoe deze incidenten zijn gecommuniceerd en opgelost;
d) de 'audit trails' van de derde partij en registraties van beveiligingsgebeurtenissen, operationele, problemen, weigeringen, opsporen van storingen en onderbrekingen verband houdend met de geleverde dienst dient minimaal eens per jaar te worden beoordeeld;
e) de verantwoordelijke manager voor het onderhouden van de relatie met een derde partij dient te controleren hoe de dienstverlener haar problemen documenteert, oplost en beheerd.

7.2.4 Wijzigingen in de SLA zijn alleen toegestaan nadat de impact van de wijziging adequaat zijn beoordeeld en indien ze schriftelijk zijn vastgelegd in een addendum bij de SLA. De verantwoordelijke vanuit de Raad dient deze wijziging formeel goed te keuren en de addendum te ondertekenen.

7.2.5 In de SLA's is het recht op audit vastgelegd. Dit houdt in dat de Raad het recht heeft om een externe audit op de diensten van de dienstverlener te laten uitvoeren.

7.3 Systeemplanning en –acceptatie

7.3.1 Capaciteitsbeheer

Doelstelling

Planvorming om te waarborgen dat de systemen nu en in de toekomst voldoende capaciteit hebben om aan de vraag te kunnen voldoen. Hiermee worden storingen als gevolg van overbelasting tot een minimum beperkt.

Richtlijnen:

7.3.1.1 Er dient een planning gemaakt te worden betreffende beoogd toekomstig gebruik inclusief een analyse van de consequenties van en voor de IT systemen door de afdeling Informatie Management om te voorkomen dat er in de toekomst te weinig computercapaciteit aanwezig is om de operaties te ondersteunen.

7.3.1.2 Twee maal per jaar wordt een knelpuntenanalyse uitgevoerd waarbij de technische prestaties van de omgeving worden onderzocht en aan het hoofd informatiemanagement gerapporteerd. Hierbij wordt tevens geanalyseerd of het verwachtte toekomstige gebruik gevolgen zal hebben voor de prestaties van de systemen (RC Verhoogd).

7.3.1.3 Indien IT beheer is uitbesteed aan een derde partij, dienen de eisen die gesteld worden aan capaciteitsplanning opgenomen te worden in de Sevice Level Agreement met desbetreffende dienstverlener.

7.3.1.4 Capaciteitswijzigingen dienen gebaseerd te zijn op tekortkomingen die worden geïdentificeerd gedurende het gebruik, of op de capaciteitsplanning.

7.3.1.5 Op ieder gewenst moment is er inzicht in systeem- en netwerkbelasting.

7.3.1.6 Periodiek wordt gerapporteerd aan de verantwoordelijk manager wat de systeem en netwerkbelasting geweest is.

7.3.2 Licentiebeheer

Doelstelling:

Door gestructureerd licentiebeheer wordt voorkomen dat de Raad te veel of te weinig licenties heeft. Hiermee worden licentierechten gerespecteerd en betaald de Raad niet te veel voor haar Software. Tevens wordt voorkomen dat de Raad maatwerksoftware kwijtraak indien de leverancier failliet gaat.

Richtlijnen:

7.3.2.1 Programmalicenties worden nageleefd.

7.3.2.2 Gebruik van illegale programmatuur is niet toegestaan.

7.3.2.3 Licentieovereenkomsten worden opgeslagen in de kluis op de afdeling IM.

7.3.2.4 Er zijn escrow-voorzieningen getroffen wat betreft bronprogrammatuur van de applicaties.

7.3.2.5 De Raad houdt een centrale administratie bij van de gekochte licenties en evalueert ten minste jaarlijks of de gekochte licenties toereikend zijn.

7.3.3 Systeemacceptatie

Doelstelling

Maatregelen dienen te waarborgen dat uitsluitend systemen in gebruik worden genomen waarvan is vast gesteld dat de functionaliteit en technische specificaties voldoen aan eisen gesteld door de gebruikers en eisen gesteld door de afdeling IM.

Richtlijnen:

7.3.3.1 De functionaliteit van een nieuw IT systeem dient te worden vastgesteld, gedocumenteerd en getest door de gebruikers in overleg met de afdeling informatiemanagement voordat het systeem wordt geaccepteerd en in gebruikgenomen.

7.3.3.2 De technische specificaties van een nieuw IT systeem dient te worden vastgesteld, gedocumenteerd en getest door de afdeling IM in overleg met de uiteindelijke gebruiker van het systeem, voordat het systeem wordt geaccepteerd en in gebruikgenomen.

7.3.3.3 De volgende punten moeten minimaal worden overwogen voordat formele acceptatie wordt verleend:

a) eisen aan functionaliteit en interoperabiliteit van het computersysteem;
b) eisen aan prestaties en capaciteit van het computersysteem;
c) procedures voor foutherstel en herstart en continuïteitsplannen;
d) voorbereiding en testen van routinematige bedieningsprocedures volgens welomschreven normen;
e) de overeengekomen beveiligingsmaatregelen zijn geïmplementeerd;
f) doeltreffende handmatige procedures;
g) bedrijfscontinuïteitsplannen;
h) bewijs dat installatie van het nieuwe systeem geen nadelige invloed heeft op bestaande systemen, in het bijzonder tijdens de drukste verwerkingstijden zoals aan het einde van de maand;
i) bewijs dat aandacht is besteed aan de invloed van het nieuwe systeem op de algehele beveiliging van de organisatie;
j) opleiding in bediening of gebruik van nieuwe systemen.
k) gebruiksgemak, omdat hiermee gebruikersprestaties worden beïnvloed en menselijk fouten wordt vermeden.

7.4 Bescherming tegen virussen en ‘mobile code’

7.4.1 Maatregelen tegen virussen

Doelstelling:

Om te voorkomen dat systemen geïnfecteerd worden met virussen, malware, wormen of enige andere vorm van ongewenste software, dienen maatregelen te worden getroffen om de IT systemen te beschermen tegen deze vormen van software.

Richtlijnen:

7.4.1.1 De medewerkers van de Raad en ingehuurde derden die werken met systemen van de Raad dienen:

a) alleen software op hun systemen installeren waarvoor de Raad een licentie heeft;
b) nieuwe of aangepaste software alleen laten installeren door personen die daartoe geautoriseerd zijn;
c) nieuw ontvangen datafiles en/of software scannen op virussen;
d) een virusscanner geïnstalleerd hebben die beschikbaar is gesteld door de Raad;

e) zorgdragen dat de virusscanner altijd aanstaat;
f) wanneer hij/zij een virus, malware, worm, etc, ontdekt, dit aan de afdeling IM meldt;
g) zorgdragen dat de virusdefinities in de virusscanner altijd up-to-date zijn.

7.4.1.2 De Raad heeft procedures waarin wordt beschreven hoe vanuit de afdeling IM wordt omgegaan met virus aanvallen. De afdeling IM is verantwoordelijk om richtlijnen en procedures te beschrijven waarin de beheersingsmaatregelen zijn beschreven waaraan iedere medewerker of ingehuurde zich moet confirmeren.

7.4.1.3 Het gebruik van macro's javascripts en VB scripts dient zoveel mogelijk te worden voorkomen. Uitsluitend mobile code van eigen applicaties is toegestaan. Maatregelen in de applicaties en in internet browsers beperken het gebruik van mobile code.

7.5 Back-up

7.5.1 Reservekopieën maken (back-ups)

Doelstelling:

Beschermen van de integriteit en beschikbaarheid van programmatuur en informatie.

Richtlijnen:

7.5.1.1 Back-ups van alle gegevens-, transactie-, autorisatie- en loggingbestanden worden gemaakt overeenkomstig de classificatie van die data en de eisen die hieraan worden gesteld door de bedrijfsvoering.

7.5.1.2 Back-up en herstelprocedures behoren regelmatig te worden gecontroleerd en getest, om te waarborgen dat ze doeltreffend zijn en dat ze kunnen worden uitgevoerd binnen de daarvoor volgens operationele herstelprocedures gestelde tijd.

7.5.1.3 Back-up tapes worden volgens een vast vervangingsschema vervangen.

7.5.1.4 De back-ups behoren te worden opgeslagen op een locatie die zich op zodanige afstand bevindt dat geen schade aan de back-up kan worden aangericht als zich een calamiteit voordoet op de hoofdlocatie.

7.5.1.5 Back-ups dienen opgeslagen te worden in afgesloten ruimtes. Voor back-ups van systemen met risico classificatie 'verhoogd' dient toegang tot deze ruimtes gelogd te worden.

7.5.1.6 In overleg met de systeemeigenaar dienen de bewaartermijnen van back-ups te worden vastgesteld.

7.5.1.7 Er dient een procedure te zijn hoe de back-ups verzameld en getransporteerd worden.

7.5.1.8 Indien back-ups voor meerdere jaren worden opgeslagen dient jaarlijks te worden vastgesteld dat deze tapes nog bruikbaar zijn.

7.5.1.9 Er dient zeker gesteld te worden dat de back-ups inderdaad potentieel dataverlies kunnen herstellen en dat deze data bruikbaar is.

7.6 Beheer van netwerkbeveiliging

Doelstelling:

De getroffen beheersingsmaatregelen beschermen het netwerk van de Raad tegen onbevoegde toegang.

Richtlijnen:

7.6.1 Maatregelen voor netwerken

7.6.1.1 De beheersingsmaatregelen die genomen dienen te worden ter bescherming van het netwerk van de Raad zijn minimaal:

- installeren van een veilig geconfigureerde firewall;

- installeren van een virusscanner (inclusief malware detectie);
- installeren van een spamfilter;
- segmenteren van het netwerk;
- invoeren van sterke authenticatie.

7.6.1.2 Externe toegang tot het netwerk van de Raad geschiedt uitsluitend met een VPN verbinding. Voor systemen met risico classificatie ‘verhoogd’ dient verbinding tot stand te komen met gebruik van sterke authenticatie (certificaat, smartcard of token).

7.6.1.3 Beheerders krijgen uitsluitend via een gecontroleerd toegangspad toegang tot de te beheren systemen.

7.6.1.4 De leverancier houdt een registratie bij om handelingen die van belang zijn voor de beveiliging te kunnen controleren. Deze vastlegging wordt maandelijks aan de afdeling IM van de Raad gezonden voor controle.

7.6.2 **Beveiliging van netwerkdiensten**

7.6.2.1 Het recht om de kundigheid van de leverancier, met de daarbij horende beveiligingsprocedures, te controleren dient in de SLA te worden beschreven.

7.6.2.2 De leverancier dient de volgende aspecten te overleggen met de Raad:

a) technologie toegepast voor de beveiliging van netwerkdiensten, zoals authenticatie, encryptie en netwerkverbindingcontroles;
b) technische parameters vereist voor beveiligde verbinding met de netwerkdiensten in overeenstemming met de beveiligings- en netwerkaansluitingsregels;
c) procedures voor het gebruik van netwerkdiensten om de toegang tot netwerkdiensten of toepassingen, waar nodig, te beperken.

7.7 Behandeling van media

Doelstelling:

Getroffen beheersingsmaatregelen waarborgen dat uitsluitend na goedkeuring van de afdeling IM gevoelige gegevens op draagbare media wordt geplaatst en dat dit wordt geregistreerd. Tevens dienen beveiligingsmaatregelen te waarborgen dat indien de draagbare media in onbevoegde handen terecht komen deze geen toegang kunnen krijgen tot gevoelige data op deze media. Gegevens die niet meer nodig zijn of media die niet meer wordt gebruikt, wordt volgens procedure verwijderd.

Richtlijnen:

7.7.1 **Beheer van verwijderbare media**

7.7.1.1 Er dienen procedures te worden opgesteld die beschrijven hoe er omgegaan dient te worden met verwijderbare media zoals tapes, USB-sticks, diskettes en harde schijven.

7.7.1.2 In principe zijn de USB-poorten van alle thin clients afgesloten voor gebruik voor USB-poorten. Data kan uitsluitend via één client per vestiging, onder verantwoordelijkheid van de lokale beheerder op draagbare media worden opgeslagen.

7.7.2 **Loggen van gebruik media**

7.7.2.1 Gebruik van draagbare media dient gelogd te worden waarbij het volgende vastgelegd wordt:

1. functionaris aan wie de media uitgeleend is;
2. beschrijving media;
3. datum uitgifte;
4. datum inname;
5. confirmatie verwijdering data.

7.7.3 **Verwijdering van media**

7.7.3.1 Indien draagbare media niet meer wordt gebruikt, dient de informatie die op het draagbare medium staat te worden verwijderd.

7.7.3.2 Indien er geen bedrijfsreden is voor gebruik van draagbare media, dient deze ingeleverd te worden.

7.7.4 **Opslaan van informatie op draagbare media**

7.7.4.1 Informatie met risico classificatie ‘verhoogd’ mag opgeslagen worden op draagbare media indien deze beveiligd is met behulp van encryptietechnologie.

7.7.5 **Beveiliging van systeemdocumentatie**

7.7.5.1 Alleen personen die daarvoor geautoriseerd zijn mogen toegang hebben tot de systeem documentatie.

7.8 Uitwisseling van informatie

Doelstelling:

Beheersingsmaatregelen waarborgen dat de integriteit en vertrouwelijkheid van elektronische gegevensuitwisseling is gewaarborgd en dat deze voldoet aan geldende wet en regelgeving.

Richtlijnen

7.8.1 **Beleid en procedures voor informatie-uitwisseling**

7.8.1.1 De Raad heeft formeel beleid, formele procedures en formele beheersingsmaatregelen vastgesteld om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen.

7.8.1.2 De Raad onderzoekt vooraf of voor de voorgenomen gegevensuitwisseling een wettelijke basis dan wel belemmering aanwezig is. Hiermee wordt ondermeer voorkomen dat de betreffende gegevensuitwisseling in strijd is met de WBP.

7.8.1.3 Met stagiairs worden specifieke afspraken gemaakt over de publicatie van onderzoeksgegevens, deze afspraken worden in de stageovereenkomst vastgelegd.

7.8.2 **Elektronisch berichtenuitwisseling**

7.8.2.1 De Raad heeft een gebruiksprotocol voor het gebruik van internet en e-mail.

7.8.2.2 Het is niet toegestaan email berichten automatisch door te sturen naar een extern e-mailadres.

7.8.2.3 Het is niet toegestaan om bedrijfsgegevens naar publieke bestandsuitwisselingssites te sturen.

7.8.2.4 Iedere medewerker die een email verstuurd namens de Raad organisatie dient een disclaimer op te nemen in iedere e-mail die verstuurd wordt naar buiten de organisatie.

7.8.2.5 Gebruikers dienen zich te confirmeren aan het e-mail- en internetprotocol. Dit protocol dient samen met een geheimhoudingsverklaring ondertekend te worden bij indiensttreding (voor derde partijen bij het inhuurcontract).

7.8.2.6 Systeemeigenaren dienen in overleg met informatiemanagement afspraken te maken over het beveiligen van elektronisch berichten verkeer.

7.8.2.7 Gegevensuitwisseling met externe partijen vindt uitsluitend plaats via een VPN tunnel.

7.8.2.8 Gegevensuitwisseling vindt uitsluitend plaats met systemen die elkaar wederzijds authenticeren.

7.8.2.9 Van ieder ontvangen informatiebericht wordt het afgesproken format gecontroleerd om zeker te zijn dat de gegevens correct zijn.

7.8.2.10 Systeemeigenaren dienen in overleg met informatiemanagement afspraken te maken over de beveiliging van publiekelijk toegankelijke data.

7.8.3 **Systemen voor bedrijfsinformatie**

7.8.3.1 Systeemdocumentatie is beschermd tegen ongeautoriseerde toegang.

7.9 Controle

Doelstelling:

De doelstelling van controle is de detectie van ongeautoriseerde toegang of transacties in de informatievoorziening.

Richtlijnen

7.9.1 **Aanmaken audit-logbestanden**

7.9.1.1 De volgende gegevens, indien relevant, dienen te worden gelogd in auditlogbestanden (RC Verhoogd):

a) gebruikers-ID's;
b) toegang tot de systemen door ‘niet-Raad’ medewerkers;
c) mislukte inlogpogingen;
d) wijzigingen van de systeemconfiguratie;
e) gebruik van speciale bevoegdheden zoals van superusers en system administrators;
f) gebruik van systeemhulpprogramma’s en -toepassingen;
g) wijzigingen in beveiligingsinstellingen;
h) wijzigingen in gebruikers en autorisaties;
i) toegang buiten kantoortijden;
j) activering en de-activering van beschermingssystemen, zoals antivirussystemen en inbraakdetectiesystemen.

7.9.2 **Controle van systeemgebruik**

7.9.2.1 De Raad heeft procedures vastgesteld om het gebruik van IT-voorzieningen door beheerders te controleren door middel van het periodiek evalueren van de logbestanden door de afdeling IM. De raad controleert of technisch beheerders onderhoudswerkzaamheden buiten de afgesproken onderhoudsintervallen hebben uitgevoerd. De resultaten hiervan worden besproken met de servicemanager.

7.9.3 **Registratie van storingen**

7.9.3.1 Voor iedere storing wordt een incidentmelding gemaakt. Deze worden geanalyseerd en tijdig worden passende maatregelen genomen.

7.9.4 **Synchronisatie van systeemklokken**

7.9.4.1 De klokken van alle relevante informatiesystemen worden gesynchroniseerd met een tijdservice.

8 Toegangsbeveiliging

8.1 Bedrijfseisen ten aanzien van toegangsbeheersing

Doelstelling:

Beheersen van de toegang van gebruikers en beheerders tot data en transacties.

8.1.1 **Toegangsbeleid**

8.1.1.1 Gebruikers worden minimaal geautoriseerd op basis van een unieke naar een individu herleidbare gebruikersnaam en een wachtwoord.

8.1.1.2 Gebruikersrechten worden, waar technisch mogelijk, toegekend op basis van rollen. Deze rollen zijn logisch geordend en zijn voldoende fijnmazig van opzet om aan de eisen van functiescheiding te kunnen voldoen. Uitgangspunt voor de opzet van rollen is: “gebruikers hebben uitsluitend rechten die expliciet worden toegekend”.

8.2 Registratie en beheer van gebruikers en hun toegangsrechten

Doelstelling

Waarborgen dat uitsluitend geautoriseerde gebruikers toegang hebben tot data en transacties.

Richtlijnen

8.2.1 **Registratie van gebruikers**

8.2.1.1 De Raad heeft formele procedures voor het registreren, wijzigen en afmelden van gebruikers en voor het verlenen, wijzigen en intrekken van toegangsrechten tot alle informatiesystemen en –diensten. Deze procedure dient ten minste de volgende elementen te bevatten:

a) controleren dat de gebruiker door de proceseigenaar is geautoriseerd voor het gebruik van het informatiesysteem of de informatiedienst;
b) controleren dat het toegewezen toegangsniveau past binnen de functie-autorisatiematrix;
c) indien **afwijkende rechten** (afwijkingen van de functie-autorisatiematrix) worden aangevraagd, dient het hoofd informatiemanagement hiervoor toestemming te verlenen. De proceseigenaar bewaakt dat deze afwijkende rechten zodra deze niet meer noodzakelijk zijn worden ingetrokken.
d) het hoofd Informatiemanagement houdt een lijst bij met gebruikers met bijzondere rechten.

8.2.1.2 De Raad heeft per applicatie een “functie-autorisatiematrix” waarin per functie is vastgelegd tot welke systemen, data en transacties personeelsleden met deze functie geautoriseerd zijn.

8.2.1.3 De functie-autorisatiematrix is goedgekeurd door de proceseigenaar. Wijzigingen op deze matrix worden door de proceseigenaar goedgekeurd. Deze wijzigingen verlopen via het reguliere formele wijzigingsproces.

8.2.1.4 Toegang tot de technische infrastructuur (servers, netwerkcomponenten en programmatuur) dienen altijd via een formeel proces te verlopen, waarbij de Securitymanager goedkeuring geeft voor de toegang. Toegang tot de technische infrastructuur en de informatiesystemen wordt gelogd en deze logging wordt periodiek gevalideerd door de afdeling informatiemanagement.

8.2.1.5 Indien gebruikers uit dienst gaan, wordt informatiemanagement hierover door de afdeling HR geïnformeerd. De afdeling informatiemanagement is er voor verantwoordelijk om gebruikers op de dag na vertrek te blokkeren in alle applicaties en in de LDAP (Active Directory). Een maand na vertrek worden gebruikers, daar waar mogelijk, definitief verwijderd door de afdeling informatiemanagement.

8.2.1.6 Regiomanagers valideren de lijst met geautoriseerde gebruikers en hun rollen periodiek en leggen de resultaten van deze controle vast. Zij rapporteren bijzonderheden aan de afdeling IM.

8.2.1.7 Gebruikers die niet meer werken voor de Raad, of langer dan 3 maanden niet actief zijn geweest, dienen automatisch verwijderd of geblokkeerd te worden (Active Directory).

8.2.2 **Beheer van gebruikerswachtwoorden**

8.2.2.1 Nieuwe gebruikers krijgen een standaard wachtwoord dat zij zelf na de eerste keer aanloggen dienen te wijzigen. Indien technisch mogelijk kunnen gebruikers pas voor de eerste keer aanloggen nadat het wachtwoord is gewijzigd.

8.2.2.2 Indien het technisch voor een bepaalde applicatie niet mogelijk is om wijzigen van het wachtwoord voor het eerste gebruik af te dwingen, verloopt het verstrekken van het eerste wachtwoord volgens een vaste procedure. Deze wachtwoorden worden uitsluitend telefonisch aan gebruikers kenbaar gemaakt.

8.2.2.3 Standaard systeemwachtwoorden (zoals admin, admin en admin, manager) dienen te worden gewijzigd.

8.3 Verantwoordelijkheden van gebruikers

Doelstelling

Gebruikers dragen zorg voor de beveiliging van gegevens door hun wachtwoorden vertrouwelijk te houden en vertrouwelijke informatie te beschermen tegen onbevoegde toegang.

8.3.1 **Gebruik van wachtwoorden**

8.3.1.1 Om zeker te stellen dat wachtwoorden niet eenvoudig kunnen worden geraden, dienen deze aan de volgende eisen te voldoen:

a) wachtwoorden dienen ten minste te bestaan uit 8 karakters,
b) wachtwoorden dienen ten minste hoofd en kleine letters te bevatten en dienen tevens of een cijfer of een speciaalteken (bijvoorbeeld !, $, # of %) te bevatten.
c) wachtwoorden dienen minimaal om de 90 dagen te worden gewijzigd;
d) wachtwoorden mogen niet twee maal in 24 uur worden gewijzigd;
e) nieuwe wachtwoorden mogen niet overeenkomen met de vorige drie gebruikte wachtwoorden;
f) wachtwoorden mogen niet overeenkomen met de gebruikersnaam;
g) wachtwoorden mogen niet leesbaar zijn opgeslagen in scripts, macro's of handleidingen.

8.3.1.2 Gebruikers nemen goede beveiligingsgewoontes in acht bij het kiezen en gebruiken van wachtwoorden. Alle gebruikers behoren:

a) wachtwoorden geheim te houden,
b) wachtwoorden niet vast te leggen (bijvoorbeeld op papier, in bestand of in handcomputer), tenzij deze registratie veilig kan worden opgeslagen en de methode van opslag is goedgekeurd,
c) wachtwoorden te wijzigen zodra er aanwijzingen zijn dat het systeem of het wachtwoord mogelijk gecompromitteerd is,
d) geen individuele gebruikerswachtwoorden met anderen te delen,
e) misbruik (of potentieel misbruik) te melden aan de hoofd informatiemanagement.

8.3.2 **'Clear desk'- en 'clear screen'-beleid**

8.3.2.1 De Raad heeft een 'clear desk'-beleid voor papier en verwijderbare opslagmedia en een 'clear screen'-beleid voor IT-voorzieningen.

8.3.2.2 Confidentiële informatie dient niet onbeheerd op de werkplaats te liggen.
8.3.2.3 Gebruikers dienen hun pc te vergrendelen bij het verlaten van de werkplek.
8.3.2.4 De Raad ondersteunt het clear-desk en clear-screen beleid actief, heeft periodieke campagnes om dit onder de aandacht van het personeel te brengen en spreekt eventuele overtreders aan op hun gedrag.

8.4 Toegangsbeheersing voor netwerken

Doelstelling

Voorkomen van ongeautoriseerde toegang tot het netwerk van de Raad.

8.4.1 Beleid ten aanzien van het gebruik van netwerkdiensten

8.4.1.1 Voor netwerkdiensten die de Raad wil leveren via het externe netwerk is een afzonderlijke DMZ omgeving ingericht. Deze DMZ is ingericht conform de eisen in het raamwerk beveiliging webapplicaties (GovCert) <http://www.govcert.nl/download.html?f=143>.
8.4.1.2 Externe toegang vindt plaats via een 2e firewall.
8.4.1.3 Indien van toepassing dient het voor de Raad mogelijk te zijn om individuen of organisaties expliciet toegang te verlenen tot de externe netwerkdiensten.
8.4.1.4 Beheeractiviteiten door leveranciers vinden uitsluitend plaats op basis van sterke authenticatie dan wel via een directe netwerkverbinding. Tevens krijgen beheerders uitsluitend toegang via een beheerst toegangspad waardoor toegang tot systemen door beheerders kan worden gelogd.
8.4.1.5 Alle internet verbindingen met het bedrijfsnetwerk van de Raad verlopen via een centraal beheerde firewall omgeving. Lokale internetverbindingen zijn losgekoppeld van het centrale netwerk.
8.4.1.6 Het interne netwerk is gesegmenteerd. Deze netwerksegmenten zijn ondermeer gebaseerd op de classificatie van systemen. Applicaties en databases met risico classificatie ‘verhoogd’ dienen afgezonderd te zijn van het operationele netwerksegment.
8.4.1.7 Op het netwerk worden uitsluitend netwerkdiensten en protocollen toegestaan die voor het primaire proces van de Raad van belang zijn.

8.5 Toegangsbeveiliging voor besturingssystemen

Doelstelling

Het voorkomen van ongeautoriseerde toegang tot de besturingssystemen van de Raad.

Richtlijnen

8.5.1 Beleid ten aanzien van de beveiliging van de Server omgeving

8.5.1.1 De IT leverancier van de Raad is ervoor verantwoordelijk te waarborgen dat toegang tot informatievoorziening plaats vindt middels afgesproken aanlog procedures. Deze verantwoordelijkheid en afspraken komen tot uitdrukking in de SLA’s en onderliggende documentatie (Dossier van afspraken en procedures).
8.5.1.2 De Raad heeft specifieke beveiligingsbaselines voor de gebruikte besturingssystemen, de IT leverancier is er voor verantwoordelijk om te waarborgen dat de inrichting van de besturingssystemen aan deze baseline voldoen.
8.5.1.3 De IT leverancier van de Raad is er voor verantwoordelijk om de toegang tot systeemprogrammatuur en configuratie bestanden te beperken en te beheersen.
8.5.1.4 Beheerders kunnen uitsluitend beheeractiviteiten uitvoeren via een zogenaamde ‘Stepping Stone’ voor het centraal monitoren en beheren van toegangsrechten van beheerders.

8.6 Toegangsbeheersing voor toepassingen en informatie

Doelstelling

Voorkomen van onbevoegde toegang tot informatie in toepassingssystemen.

8.6.1 **Richtlijnen voor toegangsbeveiliging tot applicaties**

8.6.1.1 Applicaties maken gebruik van rollen en menu's om gebruikers toegang tot gegevens te verschaffen. Deze rollen zijn dusdanig fijnmazig van opzet dat hiermee functiescheiding kan worden gewaarborgd.

8.6.1.2 Rechten behorende bij rollen en menu's in de applicaties sluiten aan bij de functie-autorisatiematrix, dit wordt jaarlijks door de afdeling Informatiemanagement gevalideerd.

8.6.1.3 Vanuit applicaties kan geen verbinding worden gelegd met beheer- en systeemontwikkel-applicaties.

8.6.1.4 De Raad heeft maatregelen getroffen om te waarborgen dat systeem output die gevoelige informatie bevat, uitsluitend die informatie bevat die noodzakelijk is voor het doel van de betreffende output.

8.6.1.5 Aanlogsystemen bewaken dat niet tegelijkertijd op verschillende desktops met dezelfde gebruiker kan worden ingelogd.

8.6.1.6 Aanlogsystemen bewaken dat een maximaal foutieve inlogpogingen is toegestaan. Indien meer dan 5 x is getracht om met een account aan te loggen wordt het betreffende account geblokkeerd.

8.6.1.7 Inactieve sessies worden na 10 minuten gedeactiveerd, werkstations zijn uitgerust met een screensaver met wachtwoord, deze is ingesteld om in te schakelen na 10 minuten inactiviteit.

8.7 Draagbare computers en telewerken

Doelstelling

Waarborgen van informatiebeveiliging bij het gebruik van draagbare computers en faciliteiten voor telewerken.

Richtlijnen

8.7.1 **Laptop gebruikers dienen zich aan de volgende regels te houden:**

a) de laptop/smartphone dient uitsluitend te worden gebruikt voor het doel waarvoor het aan de gebruiker is verstrekt;
b) de gebruiker is er voor verantwoordelijk dat steeds de laatste beveiligingsupdates van microsoft en de laatste anti-virus updates op de laptop zijn geïnstalleerd;
c) de gebruiker dient minimaal eens per 6 weken in te loggen op het interne netwerk zodoende de laatste updates en patches te downloaden en installeren;
d) de gebruiker is er zelf verantwoordelijk voor om periodiek een back-up van zijn/haar bestanden te maken;
e) de security manager dient ingelicht te worden in geval van een beveiligingsincident;
f) op alle laptops is de harde schijf encrypted;
g) de afdeling IM dient te worden benaderd in het geval van een storing;
h) de harde schijven van alle laptops zijn encrypted;
i) waarmogelijk worden smartphones voorzien van encryptie.

9 Verwerving, ontwikkeling en onderhoud van informatiesystemen

9.1 Beveiligingseisen voor informatiesystemen

Doelstelling:

Voordat een nieuw informatiesysteem wordt aangeschaft worden de functionele en technische specificaties vastgelegd en afgestemd. Hierbij worden de beveiligingseisen integraal meegenomen.

De richtlijnen in dit document zijn onverkort van toepassing op ingehuurde diensten. Bijvoorbeeld voor onderhoud en beheer van informatiesystemen. Ten tijde van het schrijven van dit document is het onderhoud en het beheer van de applicaties en en het technischbeheer van de systemen uitbesteed aan Cap Gemini en is de hosting van de systemen uitbesteed aan getronics.

Richtlijnen:

9.1.1 **Analyse en specificatie van beveiligingseisen**

9.1.1.1 Voor de bouw of aanschaf van een IT systeem, dient er een eigenaar aangewezen te worden.

9.1.1.2 Tijdens de aanschaf of ontwikkeling van een IT systeem, dient er een risicoanalyse uitgevoerd te worden door of namens de (toekomstige) proceseigenaar van het desbetreffende systeem.

9.1.1.3 De proceseigenaar dient expliciet redenen aan te geven indien er af wordt geweken van de algemeen aanvaarde beveiligingsprincipes of richtlijnen. Deze afwijkingen dienen door de security officer te worden geautoriseerd.

9.1.1.4 De leverancier of ontwikkelaar dient er zorg voor te dragen dat het nieuwe IT systeem zo optimaal mogelijk aansluit op de standaard mogelijkheden van de beveiligingsinfrastructuur.

9.2 Correcte verwerking in toepassingen

Doelstelling:

De Raad legt voor nieuwe systemen de geprogrammeerde beheersingsmaatregelen die de integriteit en vertrouwelijkheid van de gegevensverwerking dienen te waarborgen vooraf vast en bewaakt dat deze worden gerealiseerd.

Richtlijnen:

9.2.1 **Validatie van invoergegevens**

9.2.1.1 Bij de selectie of ontwerp van een nieuw IT systeem of functionaliteit, dient de eigenaar vast te stellen welke data gevalideerd dient te worden op nauwkeurigheid en volledigheid.

9.2.2 **Beheersing van interne gegevensverwerking**

9.2.2.1 Er behoren validatie controles te worden opgenomen in toepassingen om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen te ontdekken.

9.2.3 **Integriteit van berichten**

9.2.3.1 Er behoren eisen te worden vastgesteld, geschikte beheersingsmaatregelen te worden vastgesteld en geïmplementeerd voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.

9.2.4 **Validatie van uitvoergegevens**

9.2.4.1 Gegevensuitvoer uit een toepassing behoort te worden gevalideerd, om te bewerkstelligen dat de verwerking van opgeslagen gegevens op de juiste manier plaatsvindt en geschikt is gezien de omstandigheden.

9.3 Beveiliging van systeembestanden

Doelstelling:

Functiescheiding en strikte procedures zorgen ervoor dat uitsluitend geautoriseerde wijzigingen in de productiesystemen worden doorgevoerd.

Richtlijnen:

9.3.1 **Beheersing van operationele programmatuur**

9.3.1.1 Om het risico van corrumperen van productiesystemen tot een minimum te beperken behoort rekening te worden gehouden met de volgende richtlijnen om wijzigingen te beheersen:

a) het updaten van productieprogrammatuur, -toepassingen en -programmabibliotheken behoort uitsluitend te worden uitgevoerd door ervaren beheerders na goedkeuring door de directie;
b) op productiesystemen behoort alleen goedgekeurde uitvoerbare programmatuur aanwezig te zijn, geen ontwikkelcode of compilers;
c) toepassingen en besturingssysteemprogrammatuur behoren pas te worden geïmplementeerd na uitgebreide en succesvolle tests; er behoort o.a. te worden getest op bruikbaarheid, beveiliging, effecten op andere systemen en gebruikersvriendelijkheid en de tests behoren op gescheiden systemen te worden uitgevoerd; er behoort te worden gewaarborgd dat alle bijbehorende broncodebibliotheken zijn geüpdate;
d) er behoort een configuratiebeheerssysteem te worden gebruikt om alle geïnstalleerde programmatuur en de systeemdocumentatie te kunnen beheersen;
e) er behoort een terugdraaistrategie te zijn vastgesteld voordat wijzigingen worden doorgevoerd;
f) er behoort een auditlogbestand te worden bijgehouden van elke update van besturingsprogrammabibliotheken;
g) eerdere versies van de toepassingsprogrammatuur behoren te worden bewaard voor noodgevallen;
h) oude versies van programmatuur behoren te worden gearchiveerd, samen met alle vereiste informatie en parameters, procedures, configuratiedetails en ondersteunende programmatuur zolang er gegevens in het archief worden bewaard.

9.3.2 **Bescherming van testdata**

9.3.2.1 Het gebruik van operationele databases met persoonlijke informatie of enige andere gevoelige informatie voor testdoeleinden behoort te worden vermeden. Indien persoonlijke of anderszins gevoelige informatie wordt gebruikt voor testdoeleinden, behoren de testsystemen het zelfde beveiligingsniveau te hebben als de productieomgevingen. De volgende richtlijnen behoren te worden genomen ter bescherming van operationele gegevens als deze worden gebruikt bij testen:

a) testsystemen dienen in een ander netwerksegment te staan dan de operationele systemen;
b) dit netwerksegment is even goed beveiligd als de productieomgeving.

c) telkens wanneer besturingsinformatie naar een testsysteem wordt gekopieerd, behoort per keer autorisatie te worden verkregen;
d) er dient per keer dat operationele gegevens worden gebruikt, gevalideerd te worden dat de gegevens dusdanig zijn bewerkt dat deze onherkenbaar zijn geworden;
e) besturingsgegevens behoren onmiddellijk na beëindiging van de proef van het testsysteem te worden gewist;
f) kopiëren en gebruik van besturingsgegevens behoort te worden geregistreerd om in een 'audit trail' te voorzien.

9.3.3 **Toegangsbeheersing voor broncode van programmatuur**

9.3.3.1 De toegang tot broncode van programmatuur behoort te worden beperkt.

9.4 Beveiliging bij ontwikkelings- en ondersteuningsprocessen

Doelstelling:

Wijzigingsbeheer bewaakt dat uitsluitend wijzigingen worden gebouwd die door de gebruikers en de informatiemanager zijn goedgekeurd. Dat uitsluitend goed geteste en goed gedocumenteerde wijzigingen op beheerste wijze in productie worden genomen.

Richtlijnen:

9.4.1 **Procedures voor wijzigingsbeheer**

9.4.1.1 Er behoren formele procedures voor wijzigingsbeheer te worden gedocumenteerd en afgedwongen om de kans op corrumperen van informatiesystemen tot een minimum te beperken. Het invoeren van nieuwe systemen en belangrijke wijzigingen in bestaande systemen behoort een formeel proces te volgen van documentatie, specificatie, testen, kwaliteitscontrole en beheerde implementatie.

9.4.1.2 In dit proces behoort een risicobeoordeling, een analyse van de gevolgen van wijzigingen en een specificatie van de benodigde beveiligingsmaatregelen te zijn opgenomen. Dit proces behoort ook te waarborgen dat bestaande beveiliging- en beheersingsprocedures niet gecompromitteerd worden, dat ondersteunende programmeurs uitsluitend toegang wordt verleend tot die onderdelen van het systeem die ze voor hun werk nodig hebben en dat formele instemming en goedkeuring wordt verkregen voor alle wijzigingen.

9.4.1.3 Waar mogelijk behoren procedures voor wijzigingsbeheer voor toepassingsprogrammatuur en voor de operationele omgeving te worden geïntegreerd. De wijzigingsprocedures behoren de volgende punten te omvatten:

a) bijhouden van een registratie van overeengekomen autorisatieniveaus;
b) waarborgen dat wijzigingen alleen worden doorgevoerd door bevoegde gebruikers;
c) beoordelen van beheersingsmaatregelen en integriteitprocedures om te waarborgen dat deze niet door de wijzigingen gecompromitteerd worden;
d) identificatie van alle programmatuur, informatie, databases en apparatuur die wijziging behoeven;
e) vooraf verkrijgen van formele goedkeuring voor gedetailleerde voorstellen;
f) waarborgen dat bevoegde gebruikers de wijzigingen aanvaarden voordat ze worden geïmplementeerd;
g) waarborgen dat de systeemdocumentatie na elke wijziging wordt geüpdate en dat oude documentatie wordt gearchiveerd of verwijderd;
h) versiebeheer uitvoeren voor alle programmatuur-updates;

i) bijhouden van een ‘audit trail’ van alle wijzigingsaanvragen;
j) waarborgen dat de bedrijfsdocumentatie en gebruikersprocedures worden veranderd zover noodzakelijk om toepasbaar te blijven;
k) waarborgen dat de implementatie van wijzigingen op het juiste moment plaatsvindt en de betrokken bedrijfsprocessen niet verstoort.

9.4.2 **Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem**

9.4.2.1 Bij wijzigingen in besturingssystemen behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de activiteiten of beveiliging van de organisatie.

9.4.2.2 Dit proces behoort te omvatten:

a) beoordelen van de toepassingbeheersingsmaatregelen en integriteitprocedures voor de toepassing om te waarborgen dat zij niet gecompromitteerd worden door de wijzigingen in het besturingssysteem;
b) waarborgen dat in het jaarlijkse onderhoudsplan en -budget rekening wordt gehouden met beoordeling en testen als gevolg van wijzigingen in het besturingssysteem;
c) waarborgen dat wijzigingen in het besturingssysteem tijdig worden aangekondigd, zodat de noodzakelijke tests en beoordelingen kunnen worden uitgevoerd voordat de wijzigingen worden geïmplementeerd;
d) waarborgen dat de benodigde wijzigingen worden aangebracht in de bedrijfscontinuïteitsplannen.

9.4.3 **Uitbestede ontwikkeling van programmatuur**

9.4.3.1 Uitbestede ontwikkeling van programmatuur behoort onder supervisie te staan van en te worden gecontroleerd door de Raad.

9.5 Beheer van technische kwetsbaarheden

Doelstelling:

Maatregelen waarborgen dat bekende technische kwetsbaarheden tijdig worden onderkend en dat passende maatregelen worden getroffen.

Richtlijnen:

9.5.1 **Beheersing van technische kwetsbaarheden**

9.5.1.1 Er behoort tijdig informatie te worden verkregen over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie blootstaat aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen voor behandeling van daarmee samenhangende risico's.

9.5.1.2 De Raad heeft adequaat patch beleid waardoor patches voor bekende beveiligingslekken binnen afzienbare tijd worden ingevoerd.

9.5.1.3 De leverancier van de Raad levert jaarlijks en op verzoek een overzicht van alle voor de Raad beheerde configuration items aan de Raad.

10 Beheersen van informatiebeveiligingsincidenten

10.1 Beheersing van informatiebeveiligingsgebeurtenissen en zwakke plekken

Doelstelling:

Maatregelen dienen te waarborgen dat beveiligingsincidenten met de juiste prioriteit worden afgehandeld. Een beveiligingsincident is “het optreden van een gebeurtenis die ervoor zorgt of zou kunnen zorgen dat de beschikbaarheid, de exclusiviteit en/of de integriteit van de informatievoorziening wordt aangetast”.

10.1.1 Rapportage van informatiebeveiligingsgebeurtenissen

10.1.1.1 Informatiebeveiligingsgebeurtenissen worden volgens een vaste procedure in combinatie met een reactie- en escalatieprocedure voor incidenten, afgehandeld. De Raad heeft het hoofd IM aangewezen als contactpersoon voor het rapporteren van informatiebeveiligings-gebeurtenissen. Gewaarborgd behoort te zijn dat deze contactpersoon door de hele organisatie bekend is, altijd bereikbaar is (of zijn vervanging) en in staat is om passend en tijdig te reageren.

10.1.1.2 Alle werknemers, ingehuurd personeel en externe gebruikers zijn op de hoogte gebracht van hun verantwoordelijkheid om elk informatiebeveiligingsincident zo snel mogelijk te melden. Ze zijn tevens op de hoogte van de procedure voor het rapporteren van informatiebeveiligings-gebeurtenissen en van de contactpersoon. In de rapportageprocedures te zijn opgenomen:

a) feedbackprocessen om te waarborgen dat degenen die een informatiebeveiligings-gebeurtenis rapporteren ook worden geïnformeerd over de resultaten nadat de kwestie is afgehandeld;
b) formulieren voor het rapporteren van een informatiebeveiligingsgebeurtenis om het rapporteren te ondersteunen en om degene die rapporteert te helpen herinneren aan alle noodzakelijke handelingen in het geval van een informatiebeveiligingsgebeurtenis;
c) het juiste gedrag in het geval van een informatiebeveiligingsincident, d.w.z.:
    i. onmiddellijk noteren van alle belangrijke details (bijvoorbeeld soort niet-naleving of beveiligingslek, optredende storing, schermboodschappen, vreemd gedrag);
    ii. zelf geen enkele actie ondernemen, maar onmiddellijk rapporteren aan de contactpersoon;
d) verwijzing naar een vastgesteld formeel disciplinair proces voor het omgaan met werknemers, ingehuurd personeel of externe gebruikers die de beveiliging doorbreken.

10.1.1.3 Waar een vervolgprocedure tegen een persoon of organisatie na een informatiebeveiligingsincident juridische maatregelen omvat (civiel of strafrechtelijk), wordt bewijsmateriaal verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

11 Beheerproces bedrijfscontinuïteit

11.1 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

Doelstelling:

De Raad heeft informatiebeveiligingsmaatregelen getroffen om te waarborgen dat in geval van een incident het dataverlies niet meer bedraagt dan 24 uur. Tevens heeft de Raad maatregelen getroffen om te waarborgen dat ingeval van incidenten de IT dienstverlening binnen een maximale wachttijd weer wordt hersteld.

De maximale gegevensverlies en –hersteltijden in geval van incidenten zijn:

	Basis	Verhoogd
Max. gegevensverlies	24 uur	24 uur
Max. hersteltijd	48 uur	24 uur

Voor calamiteiten zoals brand, terroristische aanvallen, milieurampen of het instorten van het gebouw heeft de Raad geen aanvullende maatregelen getroffen ten aanzien van de maximale herstel tijd. Ook voor de back-ups geldt dat een maximaal gegevensverlies voor deze gevallen niet aanvullend wordt geborgd.

Richtlijnen:

11.1.1 Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer

11.1.1.1 De Raad heeft een beheerd proces voor bedrijfscontinuïteit in de gehele organisatie ontwikkeld, voor de naleving van eisen voor informatiebeveiliging die nodig zijn voor de continuïteit van de bedrijfsvoering. In dit proces zijn de volgende aandachtspunten te worden vastgelegd:

a) de kritieke processen waarvoor het plan geldt;
b) de impact van het wegvallen van deze processen voor de bedrijfsvoering;
c) een escalatie plan (wanneer wordt overgegaan tot welke maatregelen en wie bepaalt wanneer welk escalatieplan in werking treed);
d) geprinte versies van de calamiteitenplannen en contactenlijsten dienen aanwezig te zijn;
e) handmatige procedures om de periode van uitval zoveel mogelijk op te vangen;
f) herstel van de dienstverlening met behoud van synchroniteit tussen de systemen.

11.1.2 Testen, onderhoud en herbeoordelen van bedrijfscontinuïteitsplannen

11.1.2.1 Bedrijfscontinuïteitsplannen worden regelmatig getest en geüpdate, om te bewerkstelligen dat ze actueel en doeltreffend blijven.

12 Naleving

12.1 Naleving van wettelijke voorschriften

Doelstelling:

Beheersingsmaatregelen waarborgen dat geldende wet- en regelgeving en het informatiebeveiligings-beleid worden nageleefd.

Richtlijnen:

12.1.1 **Identificatie van toepasselijke wetgeving**

12.1.1.1 De Raad heeft de geldende wettelijke en regelgevende eisen vertaald naar concrete beheersingsmaatregelen en deze vastgelegd in het beveiligingsraamwerk.

12.1.1.2 De Raad ziet er jaarlijks op toe dat deze maatregelen nog actueel zijn.

12.1.2 **Bescherming van bedrijfsdocumenten**

12.1.2.1 Documenten met betrekking tot zaken die in de primaire processen worden verzameld worden in het elektronische documentmanagement systeem opgeslagen.

12.1.2.2 De Raad heeft passende beveiligingsmaatregelen getroffen om de integriteit, vertrouwelijkheid en continuïteit van deze registratie te waarborgen .

12.1.3 **Voorkomen van misbruik van IT-voorzieningen**

12.1.3.1 De directie keurt het gebruik van IT-voorzieningen goed voordat deze in gebruik worden genomen.

12.1.3.2 Gebruik van IT voorzieningen voor niet-zakelijke doeleinden zonder toestemming van de directie of voor enig onbevoegd doel behoort te worden beschouwd als onoorbaar gebruik van de voorzieningen. Indien enige ongeautoriseerde activiteit wordt gesignaleerd door middel van controle of anderszins, behoort deze activiteit onder de aandacht te worden gebracht van de desbetreffende manager om te overwegen of disciplinaire en/of juridische maatregelen kunnen worden getroffen.

12.1.3.3 Alle gebruikers zijn op de hoogte van de exacte reikwijdte van hun toegangsrechten en van het feit dat gecontroleerd wordt om onbevoegd gebruik te ontdekken.

12.1.3.4 Werknemers van de organisatie, ingehuurd personeel en externe gebruikers behoort te worden gemeld dat geen toegang zal worden toegestaan met uitzondering van geautoriseerde toegang.

12.2 Naleving van beveiligingsbeleid en -normen en technische naleving

12.2.1 **Naleving van beveiligingsbeleid en -normen**

12.2.1.1 Managers behoren te bewerkstelligen dat alle beveiligingsprocedures die binnen hun verantwoordelijkheid vallen correct worden uitgevoerd om naleving te bereiken van beveiligingsbeleid en -normen.

12.2.1.2 De raad behoort regelmatig te beoordelen of de informatieverwerking binnen de Raad voldoet aan het geldende beveiligingsbeleid, normen en andere beveiligingseisen.

12.2.1.3 Indien als resultaat van de beoordeling een geval van niet-naleving wordt ontdekt, behoren de verantwoordelijke managers:

a) de oorzaken van deze niet-naleving vast te stellen;
b) de noodzaak voor handelen te beoordelen om te waarborgen dat niet-naleving zich niet opnieuw voordoet;
c) passende corrigerende maatregelen vast te stellen en te implementeren;

d) de uitgevoerde correctieve maatregel beoordelen.

12.2.1.4 De resultaten van de beoordelingen van audits en reviews en de corrigerende handelingen die door managers zijn uitgevoerd, behoren te worden geregistreerd en deze registraties behoren te worden bewaard. De managers behoren wanneer de onafhankelijke beoordeling plaatsvindt in hun verantwoordelijkheidsgebied de resultaten te rapporteren aan de personen die de onafhankelijke beoordelingen uitvoeren.

12.2.2 **Controle op technische naleving**

12.2.2.1 Informatiesystemen behoren regelmatig te worden gecontroleerd op naleving van implementatie van Beveiligingsnormen.

12.3 Overwegingen bij audits van informatiesystemen

12.3.1 **Beheersingsmaatregelen voor audits van informatiesystemen**

12.3.1.1 Eisen voor audits en andere activiteiten waarbij controles worden uitgevoerd op productiesystemen, behoren zorgvuldig te worden gepland en goedgekeurd om het risico van verstoring van bedrijfsprocessen tot een minimum te beperken.

12.3.2 **Bescherming van hulpmiddelen voor audits van informatiesystemen**

12.3.2.1 Toegang tot hulpmiddelen voor audits of reviews van informatiesystemen behoort te worden beschermd om mogelijk misbuik of compromittering te voorkomen.

Bijlage I Richtlijnen voor classificatie conform de WBP

Beveiliging persoonsgegevens
Artikel 13 WBP legt op de verantwoordelijke voor een verwerking (registratie) van persoonsgegevens een verplichting tot beveiliging van die persoonsgegevens op:

"De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen."

De verplichting tot beveiliging van de persoonsgegevens in art. 13 WBP tegen verlies of tegen enige vorm van onrechtmatige verwerking heeft betrekking op alle onderdelen waarbinnen persoonsgegevens worden verwerkt.

De door de verantwoordelijke te nemen beveiligingsmaatregelen zijn afhankelijk van de aard en omvang van de persoonsgegevens en van de wijze van verwerking van die persoonsgegevens. Door de verantwoordelijke dient een analyse te worden uitgevoerd teneinde te bepalen welke risicoklasse van toepassing is op de persoonsgegevens.

Conform de eisen van De Registratiekamer gaat de Raad uit van vier risicoklassen. De opbouw van de risicoklassen is cumulatief: hogere klassen geven additionele normen aan die passen bij de hogere risicoklasse. De vier risicoklassen die in ieder geval kunnen worden onderscheiden zijn:

Risicoklasse 0: publiek niveau
Het gaat hier om openbare persoonsgegevens. In deze klasse zijn persoonsgegevens opgenomen waarvan algemeen aanvaard is dat deze, bij het beoogde gebruik, geen risico opleveren voor de betrokkene. Voorbeelden hiervan zijn telefoonboeken, brochures, publieke internetsites, etc. De persoonsgegevens behoeven ten aanzien van de exclusiviteit van de persoonsgegevens niet beter beveiligd te worden dan gebruikelijk is om een toereikende kwaliteit van de informatievoorziening tot stand te brengen en in stand te houden. Als gevolg van de Wet bescherming persoonsgegevens worden voor deze risicoklasse geen extra eisen ten aanzien van de beveiliging gesteld dan welke al noodzakelijk zijn voor een zorgvuldige bedrijfsvoering.

Risicoklasse I: basisniveau
De risico's voor de betrokkene bij verlies of onbevoegd of onzorgvuldig gebruik van de persoonsgegevens zijn zodanig dat standaard (informatie)beveiligingsmaatregelen toereikend zijn. Bij verwerkingen van persoonsgegevens in deze klasse gaat het meestal om een beperkt aantal persoonsgegevens dat betrekking heeft op bijvoorbeeld lidmaatschappen, arbeidsrelaties, klantrelaties en overeenkomstige relaties tussen een betrokkene en een organisatie.

Voorbeelden van relaties waarover veelal persoonsgegevens worden verwerkt die vallen in deze klasse zijn: school - leerling, verhuurder - huurder, hotel - gast, vereniging - lid, organisatie - deelnemer.
In deze klasse zijn de risico's zodanig dat met een basispakket van beveiligingsmaatregelen kan worden volstaan.

Risicoklasse II: verhoogd risico
In deze klasse bestaan extra risico's voor negatieve gevolgen voor de betrokkenen bij onbevoegd of onzorgvuldig gebruik van persoonsgegevens. De verwerkingen van bijzondere (gevoelige) gegevens als bedoeld in art. 16 van de Wet bescherming persoonsgegevens vallen in ieder geval in deze risicoklasse.

Binnen dit niveau valt bijvoorbeeld de verwerking in het bank- en verzekeringswezen van gegevens over de persoonlijke of economische situatie van een betrokkene of de verwerking van gegevens bij handelsinformatiebureaus ten behoeve van kredietinformatie of schuldsanering. Ook verwerkingen die hiermee vergelijkbaar zijn, zoals de verwerking van financiële gegevens door de Raad, vallen onder risicoklasse II.

Risicoklasse III: Hoog risico
In deze klasse is sprake van verwerking van persoonsgegevens die in aanmerkelijke mate een risico opleveren voor onbevoegd of onzorgvuldig gebruik. Dit geldt bijvoorbeeld bij verwerking van meerdere verzamelingen van bijzondere persoonsgegevens. Ook wanneer een bijzondere geheimhoudingsplicht van toepassing is op de persoonsgegevens vallen deze onder risicoklasse III.

De beveiligingsmaatregelen die voor de beveiliging van dergelijke persoonsgegevens moeten worden genomen, moeten voldoen aan de hoogste normen. De gegevensdrager (CD-ROM, tapes, schijven, intern geheugen) van persoonsgegevens die onder deze risicoklasse vallen, moet – voor dat zover technisch mogelijk is – worden voorzien van een markering waaruit direct blijkt dat deze gegevens in risicoklasse III vallen. In de Achtergrondstudie en Verkenningen nr. 23 van de Registratiekamer wordt gedetailleerd weergegeven welke beveiligingseisen er gelden bij risicoklasse III.

De verantwoordelijke is verplicht te zorgen voor een niveau van beveiliging van de persoonsgegevens dat overeenkomt met de eisen die in het rapport van de Registratiekamer worden gepresenteerd. Als er sprake is van een bewerker in de zin van de wet (artikel 14 WBP; zie paragraaf 3.5), dient de verantwoordelijke die bewerker te instrueren over de wijze waarop de persoonsgegevens moeten worden beveiligd. De uiteindelijke keuze van het stelsel van algemene maatregelen wordt bepaald door de 'state of the art', de kosten van de maatregelen en de continuïteit van bepaalde voorzieningen. De verantwoordelijke dient een evenwichtige afweging te maken tussen deze factoren en het belang van de beveiliging van de persoonsgegevens en hij dient deze afweging te documenteren. Het uit deze afweging voortvloeiende beveiligingsstelsel behoort permanent een evenwichtig stelsel van zowel technische als organisatorische maatregelen te zijn.

Volgens de eisen van de Registratiekamer is de verantwoordelijke verplicht met de volgende aspecten van informatiebeveiliging rekening te houden:

1. vaststellen van beveiligingsbeleid, beveiligingsplan en implementatie van het stelsel van maatregelen en procedures;
2. administratieve organisatie (beschrijving) van de beveiliging;
3. bevorderen van beveiligingsbewustzijn;

4. eisen stellen bij werving en selectie van personeel;
5. juiste inrichting van de werkplek;
6. beheer en classificatie van de ICT infrastructuur;
7. toegangsbeheer en –controle;
8. beveiliging van netwerken en externe verbindingen;
9. voorwaarden aan het gebruik van software van derden;
10. beveiliging bij bulkverwerking van persoonsgegevens;
11. eisen aan het bewaren van persoonsgegevens;
12. eisen aan de vernietiging van persoonsgegevens;
13. opstellen van een calamiteitenplan;
14. aandacht voor beveiliging bij uitbesteden van en overeenkomsten voor de verwerking van persoonsgegevens.

Voor de verwerking van cliëntgegevens in de informatiesystemen van de Raad betekent dit bijvoorbeeld dat:

- de gegevensverwerking (opslag en transport) zoveel mogelijk versleuteld dient te zijn;
- identificatie en verificatie dienen adequaat geregeld te zijn;
- er dient sprake te zijn van een strikte autorisatie: alleen degenen die daartoe bevoegd zijn mogen toegang hebben tot de gegevens in het systeem.

Wat de versleuteling betreft stelt de Registratiekamer dat in ieder geval moet worden voorkomen dat berichten met persoonsgegevens zonder expliciet, bewust handelen, ongeoorloofd worden gelezen door onbevoegde personen. Voor de uitwisseling van persoonsgegevens in risicoklasse III geldt bijvoorbeeld dat:

- de verantwoordelijke uitsluitend datacommunicatie toepast over netwerken buiten het toezicht van zijn eigen organisatie, indien hij expliciete waarborgen (zekerheden) heeft over de kwaliteit van de geïmplementeerde beveiligingsmaatregelen;
- de verzender het berichtenverkeer zodanig vastlegt dat achteraf vastgesteld kan worden wanneer en aan wie een bericht met persoonsgegevens is verzonden en treft voorzieningen voor een vergelijkbare functionaliteit voor de ontvangen berichten;
- de verzender van een bericht (systeem of gebruiker) zich ervan vergewist dat een getransporteerd bericht ongewijzigd is overgebracht.

Het vereiste van integriteit heeft betrekking op de kwaliteit van de verwerkte persoonsgegevens. Deze dienen in het algemeen juist, volledig en actueel te zijn. Hiertoe moeten maatregelen worden getroffen die kunnen waarborgen dat de gegevens juist en nauwkeurig zijn, gelet op de doeleinden waarvoor ze zijn verzameld.

Het vereiste van beschikbaarheid houdt in dat de persoonsgegevens steeds beschikbaar moeten zijn overeenkomstig daarover gemaakte afspraken en wettelijke voorschriften. Wettelijke voorschriften bestaan bijvoorbeeld om (persoons)gegevens in boeken, bescheiden en andere gegevensdragers gedurende 7 jaar te bewaren op grond van art. 2:10 en 3:15i BW en art. 52 Algemene wet inzake de rijksbelastingen.

Bijlage II Nadere toelichting op de kaders voor de informatiebeveiliging van de Raad

Wet Bescherming Persoonsgegevens (WBP)

De Wet Bescherming Persoonsgegevens (WBP) gaat over persoonsgegevens, zoals die op grote schaal worden verwerkt door overheid, bedrijven en andere organisaties. Deze wet stelt normen voor een behoorlijke en zorgvuldige verwerking van persoonsgegevens. Een belangrijk element is dat passende technische en organisatorische maatregelen worden getroffen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.

Voor de beveiliging van persoonsgegevens heeft het College Bescherming Persoonsgegevens een handreiking opgesteld om te kunnen voldoen aan de voorschriften uit de WBP. Daarin worden vier risicoklassen onderscheiden en worden per risicoklasse passende maatregelen aangegeven.

Kortom, ook vanuit de WBP wordt gesteld dat er passende beveiligingsmaatregelen moeten worden getroffen rekening houdend met de beveiligingsrisicoklasse (beveiligingseisen).

De informatiesystemen van de Raad bevatten zogenaamde bijzondere persoonsgegevens waarvoor geldt dat: extra negatieve gevolgen bestaan voor de betrokkene bij verlies, onbehoorlijke of onzorgvuldige verwerking van de persoonsgegevens. Gegevens worden hiermee in termen van de WBP geclassificeerd in '**risicoklasse II**'. Binnen de risico classificatie van de Raad is dit vertaald of gelijkgesteld aan '**verhoogd**' risico.

Besluit voorschrift informatiebeveiliging rijksdienst 2007 (VIR)

De ministeriële kaders waaraan zal moeten worden voldaan is het Besluit voorschrift informatie-beveiliging rijksdienst 2007 (VIR). Dit besluit legt in artikel 4 de volgende verantwoordelijkheden vast voor het lijnmanagement van de Raad.

> *Artikel 4. VIR Verantwoordelijkheden lijnmanagement*
> *Het lijnmanagement is verantwoordelijk voor de beveiliging van zijn informatiesystemen. Het lijnmanagement:*
> a. *Stelt op basis van een expliciet risico afweging de betrouwbaarheidseisen voor zijn informatiesystemen vast;*
> b. *Is verantwoordelijk voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;*
> c. *Stelt vast dat de getroffen maatregelen aantoonbaar overeenstemmen met de betrouwbaarheidseisen en dat deze maatregelen worden nageleefd;*
> d. *Evalueert periodiek het geheel van betrouwbaarheidseisen en beveiligingsmaatregelen en stelt deze waar nodig bij.*

Op basis van een risicoanalyse zijn de betrouwbaarheidseisen geformuleerd en vertaald naar maatregelen.

Raamwerk Beveiliging Webapplicaties

Het Govcert is de overheidsinstelling die zich bezighoudt met het bewaken van het Nederlandse Internetverkeer en heeft een document met beveiligingsmaatregelen opgesteld waaraan websites van overheidsinstellingen in de basis aan zouden moeten voldoen, het Raamwerk Beveiliging Web-applicaties.

Bijlage III Indeling van gegevensstromen naar beveiligingsniveaus

In onderstaande tabellen is per gegevensstroom voor ieder relevant kwaliteitsaspect het gewenste beveiligingsniveau weergegeven.

Gegevensstroom	Gegevens	Integriteit	Continuïteit	Vertrouwelijkheid
Aanvragen via webportaal/poststukken in de postkamer	– Persoonsgegevens rechtzoekende – Gezinssamenstelling – N.A.W. gegevens rechtsbijstandverleners – Zaakgegevens – Inkomensgegevens – Declaratiegegevens	Verhoogd	Verhoogd	Verhoogd
Dossiers binnen Workflow Management	– Dossier nummer – Status – Behandelaar – Processtuur informatie	Verhoogd	Verhoogd	Basis
Dossiers in Gras	– Persoonsgegevens rechtzoekende – Gezinssamenstelling – N.A.W. gegevens rechtsbijstandverleners – Zaakgegevens – Inkomensgegevens – Declaratiegegevens – Beslisgegevens – Piketrooster	Verhoogd	Verhoogd	Verhoogd
Documenten en records met betrekking tot dossiers in het Document Management Systeem	– Persoonsgegevens rechtzoekende – Gezinssamenstelling – N.A.W. gegevens rechtsbijstandverleners – Zaakgegevens – Inkomensgegevens – Declaratiegegevens – Beslisgegevens	Verhoogd	Verhoogd	Verhoogd
GCS	– Document templates	Basis	Verhoogd	Basis

Gegevensstroom	Gegevens	Integriteit	Continuïteit	Vertrouwelijkheid
RIS	– Advocaat/mediator –en kantoorgegevens Verwijsarrangementen (rechtsgebieden) – Bankrekeningnummers – E-mail adressen – Mobiel nummers	Verhoogd	Basis	Verhoogd
Teamsoft (Open Finance)	– Programma kosten – Apparaatskosten – Debiteuren gegevens – Crediteuren (Advocaat/mediator- en persoonsgegevens, persoonsgegevens rechtzoekenden) – Financiële administratie	Verhoogd	Basis	Verhoogd
Berichtenmakelaar (MQ Soniq), afhandeling van interfaces met externe bronnen	– Persoonsgegevens – Gegevens omtrent de rechtsbijstandverlener – Inkomensgegevens – Verwijsarrangementen (rechtsgebieden) – Advocaat/mediator –en kantoorgegevens	Basis	Verhoogd	Verhoogd
Interface Webstar tussen Gras en het Juridisch Loket	– Advocaat/mediator –en kantoorgegevens Verwijsarrangementen	Basis	Basis	Basis
Interface tussen Gras en TeamSoft	– Debiteuren en crediteuren gegevens – Financiële gegevens	Basis	Basis	Basis
Interface tussen Gras en GCS	– Persoonsgegevens rechtzoekende – Gezinssamenstelling – N.A.W. gegevens rechtsbijstandverleners – Zaakgegevens – Inkomensgegevens – Declaratiegegevens – Beslisgegevens	Basis	Verhoogd	Verhoogd
Interface tussen Gras en Webstar naar het Webportaal	– Advocaat/mediator –en kantoorgegevens	Basis	Basis	Basis