REGIONALE BELASTING GROEP

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 156

26 januari 2026

Officiële uitgave van de gemeenschappelijke regeling Regionale Belasting Groep

Informatiebeveiligingsbeleid Regionale Belasting Groep

1. Inleiding

1.1 Aanleiding

De steeds grotere afhankelijkheid van informatiesystemen en informatiestromen leidt tot voelbare risico's voor de continuïteit van de dienstverlening van de Regionale Belasting Groep (RBG). Voor onze processen is het van cruciaal belang om over informatie(systemen) te beschikken die voldoen aan de gestelde eisen (vertrouwelijkheid, integriteit of beschikbaarheid). 99 procent van alle informatie binnen de RBG is digitaal beschikbaar en wordt digitaal uitgewisseld. Opslag van deze gegevens is voor 99 procent in de Cloud. Laptops, tablets en mobiele telefoons die via het internet verbonden worden met bedrijfsapplicaties waarmee op een efficiëntie wijze gecommuniceerd kan worden en eenvoudig informatie kan worden uitgewisseld.

De afgelopen jaren neemt het aantal incidenten rondom informatiebeveiliging toe. Wereldwijd is er een toename in cyberaanvallen met ransomware. Overheden, banken, havenbedrijven en andere grote organisaties zijn getroffen door deze aanvallen.
De financiële gevolgen van een dergelijke aanvallen zijn groot, de imagoschade enorm. De toenemende cybercrime heeft de Tweede Kamer en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) er toe gebracht alle overheden te vragen maatregelen te nemen die de digitale veiligheid garanderen. Zoals reeds aangegeven is ook voor de RBG het beschikbaar hebben en houden van de verschillende informatiesystemen van groot belang.

Daarnaast is er wet- en regelgeving die de Regionale Belasting Groep verplicht maatregelen te treffen om te voorkomen dat informatie/gegevens gemanipuleerd worden, onbevoegd worden bekeken, verwijderd worden of informatiesystemen uitvallen. Voorbeelden zijn de Algemene Verordening Gegevensbescherming (AVG) en de Baseline Informatie Beveiliging Overheid (BIO).

1.2 Doel van informatiebeveiliging

Het informatiebeveiligingsbeleid heeft als doel om kaders te scheppen waarbinnen de werking van onze systemen en van de (geautomatiseerde) uitwisseling van informatie van en naar onze organisatie op een betrouwbare manier wordt ingericht. Hiermee trachten we de beschikbaarheid, de integriteit en de vertrouwelijkheid van onze informatiesystemen en van de (geautomatiseerde) gegevensuitwisseling te waarborgen. Deze kaders zijn niet alleen van toepassing op onze informatiesystemen maar ook op de beveiliging van niet digitale gegevensdragers en de fysieke beveiliging van ons gebouw en onze medewerkers.

1.2.1 Geformuleerde kaders

1. Informatiebeveiliging is niet alleen een technisch onderwerp voor de afdeling ICT. Het belang van informatiebeveiliging zal bij alle medewerkers (en managers) bekend moeten zijn.
2. Binnen de opleidingen van de RBG-academie wordt de nodige aandacht besteed aan informatiebeveiliging. Dit thema dient een terugkerend onderwerp te zijn binnen de opleidingen.
3. Informatiebeveiligingsbeleid sluit aan op het strategisch kader zoals vastgelegd in de Baseline Informatiebeveiliging Overheid (BIO).
4. Maatregelen in het kader van Informatiebeveiliging worden genomen op basis van een risico of knelpuntenanalyse.
5. Handhaving van de informatiebeveiliging is een verantwoordelijkheid van de lijnmanagers; de CISO ondersteunt hierbij.
6. Informatiebeveiliging draagt bij aan het operationeel houden van de bedrijfsprocessen. Het is geen doel op zich zal altijd in evenwicht zijn met klantgericht- en efficiënt werken.
7. Alle processen en informatiesystemen hebben een formele eigenaar binnen de organisatie.
8. Alle noodzakelijke maatregelen worden genomen om te voldoen aan wet- en regelgeving op het gebied van informatiebeveiliging.
9. Daar waar afgeweken wordt van vastgesteld beleid of standaarden, legt het management dit vast in een formele verklaring.
10. Een medewerker beschikt over de informatie die hij voor zijn functie nodig heeft. Door middel van een gebruikersnaam en wachtwoord wordt binnen de informatiesystemen functiescheiding toegepast.

1.3 Scope

Informatiebeveiliging is niet alleen een technisch onderwerp voor de afdeling ICT. Het gaat om:

- alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis)
- alle mogelijke informatiedragers (papier, elektronisch, foto, film, CD, DVD, USB, SD kaart, beeldscherm et cetera)
- alle informatie verwerkende systemen (applicaties, systeemprogrammatuur, netwerken, databases, hardware, bijbehorende bedrijfsmiddelen)
- toegang tot gebouw en ruimtes
- het gebruik van apparatuur
- maar vooral ook om menselijk handelen en processen.

De meeste incidenten komen niet voort uit gebrekkige techniek, maar vooral door menselijk handelen en het tekort schieten van de bewustwording in de organisatie.
De scope van het informatiebeveiligingsbeleid omvat dan ook alle bedrijfsfuncties, ondersteunende middelen en informatie van de RBG in de meest brede zin van het woord. Het beleid is ook van toepassing op alle ruimten van het kantoorpand, de apparatuur, programmatuur en alle informatie/gegevens die de Regionale Belasting Groep gebruikt.

2. Organisatie van informatiebeveiliging en privacy

Het bestuur en management spelen een belangrijke rol binnen het informatiebeveiligingsbeleid. Zo maakt het management een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de RBG heeft, de risico's die de RBG hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan maakt het management beleid voor informatiebeveiliging, draagt dit uit naar de organisatie en bewaakt de uitvoering hiervan.

Het management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt door het uitbrengen en handhaven van dit beleid. Het beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het algemene beleid en de relevante landelijke en Europese wet- en regelgeving.

De RBG is zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van het beleid. Hierbij geldt:

- Er is wetgeving waar altijd aan voldaan moet worden, zoals (niet uitputtend) bijvoorbeeld BSN, BAG, maar ook de archiefwet.
- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Overheid (BIO).

2.1 Verantwoordelijke functionarissen

Periodiek wordt in het managementoverleg informatiebeveiliging en informatiebeheer besproken. De clustermanagers zijn verantwoordelijk voor de handhaving van het beleid binnen hun cluster en dragen zorg voor een groot deel van de uitvoering van het geformuleerde beleid.

2.1.1 CISO

Bij de RBG is de Chief Information & Security Officer (CISO) als functie opgenomen in het functieboek en ingevuld. De CISO rapporteert rechtstreeks aan de controller/plaatsvervangend directeur en ondersteunt en adviseert de clustermanagers.

De CISO bevordert en adviseert gevraagd en ongevraagd over de beveiliging van de RBG, verzorgt rapportages over de status, draagt zorg voor controle op de beveiliging van de RBG en controleert of de maatregelen worden nageleefd, evalueert de uitkomsten en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de informatiebeveiliging.

Bij een beveiligingsincident wordt contact opgenomen met de autoriteiten Informatiebeveiligingsdienst (IBD). De CISO is verantwoordelijk voor de contacten en vastlegging van deze incidenten.

2.2 Privacybescherming

Naast informatiebeveiliging is ook privacybescherming van groot belang. De Algemene Verordening Gegevensbescherming biedt organisaties ruimte om een Privacy Officer (PO) aan te stellen. De AVG eist van overheidsorganisaties dat zij beschikken over een Functionaris Gegevensbescherming (FG).

2.2.1 Functionaris Gegevensbescherming

Op basis van de huidige Europese privacy verordening (AVG), die in mei 2018 van kracht is geworden, zijn alle overheidsorganisaties verplicht een FG aan te stellen. De FG is verantwoordelijk voor het toezicht houden op de naleving van de privacywetten en -regels, het inventariseren en bijhouden van gegevensverwerkingen en het afhandelen van vragen en klachten van mensen binnen en buiten de organisatie.

Daarnaast kan de FG ondersteunen bij het ontwikkelen van interne regelingen, het adviseren over privacy op maat én het leveren van input bij het opstellen of aanpassen van gedragscodes.
Het registratienummer van de Autoriteit Persoonsgegevens, van de aangestelde FG, is opgenomen in het personeelsdossier.

Indien er sprake is van een datalek dan neemt de Functionaris Gegevensbescherming (FG) contact op met de Autoriteit Persoonsgegevens (AP).

2.2.2 Privacy Officer

Waar de CISO verantwoordelijk is voor het informatiebeveiligingsbeleid is de Privacy Officer (PO) verantwoordelijk voor het vormgeven en bewaken van het privacy beleid binnen de organisatie. Daarnaast kan de PO ondersteunen bij het in kaart brengen van de risico's door bijvoorbeeld een Data Protection Impact Assessment (DPIA) uit te voeren. Een DPIA kan resulteren in het aanpassen van zaken. Hiervoor wordt een implementatieplan opgesteld en uitgevoerd door de PO. Daarnaast speelt de PO ook een belangrijke rol op de werkvloer. Zo heeft hij net als de CISO een adviserende rol richting de vak afdelingen en kan hij of zij vragen beantwoorden zoals: hoe moeten we deze gegevens delen? Aan welke regels dienen we ons te houden? Welke maatregelen moeten we de externe partij opleggen?

De Regionale Belasting Groep heeft functionarissen aangesteld voor:

- Chief Information & Security Officer
- Functionaris Gegevensbescherming
- Privacy Officer

3. Uitwerking beleid

Jaarlijks wordt op basis van het beveiligingsbeleid een risico of knelpunten analyse uitgevoerd op binnen de scope vallende onderdelen. Naar aanleiding van de geconstateerde knelpunten wordt een uitvoeringsplan (informatiebeveiligingsplan) opgesteld. Hierin wordt de implementatie van het beleid, richtlijnen, procesbeschrijvingen, procedures en technische maatregelen met betrekking tot informatiebeveiliging beschreven. De implementatie en handhaving hiervan is de verantwoordelijkheid van de clustermanagers.

Verantwoordelijke	**Relevantie voor Informatiebeveiligingsbeleid**
Dagelijks Bestuur	Integrale verantwoordelijkheid
Management Team	Kaderstelling en implementatie
Clustermanagers	Sturing op informatieveiligheid en controle op naleving
Alle medewerkers	Gedrag en naleving
Proces en gegevenseigenaren	Bepalen van de beschermingseisen van informatie op basis van data classificatie
het management team	Planvorming binnen de informatiebeveiligingskaders
CISO	Algemene en dagelijkse coördinatie van de informatiebeveiliging, adviseren over de implementatie van het informatiebeveiligingsbeleid
Personeelszaken	Arbeidsvoorwaardelijke zaken
Facilitaire zaken	Fysieke toegangsbeveiliging
het team ICT	Technische beveiliging
Auditors (intern / extern)	Onafhankelijke toetsing van het beleid
Leveranciers en ketenpartners	Voldoen aan het beleid van de RBG

Visie

De RBG zet continue in op het verhogen van informatieveiligheid en verdere professionalisering van de informatiebeveiligingsfunctie in de organisatie. Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de RBG en de basis voor het beschermen van rechten van burgers en bedrijven.

Het proces van informatiebeveiliging is primair gericht op bescherming van informatie en stimuleert daarnaast ontwikkelingen op dit gebied. Het maakt bijvoorbeeld elektronische dienstverlening op verantwoorde wijze mogelijk evenals nieuwe en innovatieve manieren van werken.
De focus is informatie uitwisselen in alle verschijningsvormen, zoals elektronisch, op papier en mondeling. Het gaat ook niet alleen over ICT: verantwoord en bewust gedrag van alle medewerkers is essentieel voor informatieveiligheid.

Informatiebeveiliging is een integraal onderdeel van de reguliere werkwijze binnen de RBG. Informatiebeveiligingsaspecten worden derhalve in alle procesbeschrijvingen en werkinstructies opgenomen.

3.1 Beleidsproces

Het proces om beveiligingsbeleid vast te stellen en hier uitvoering aan te geven verloopt volgens het principe van: Plan -> Act -> Check –> Do

Plan	:	Wet- en regelgeving Landelijke normen Baseline Informatiebeveiliging Overheid (BIO) Vaststellen informatiebeveiligingsbeleid
Act	:	Risicoanalyses Informatiebeveiligingsplan Nulmeting of vervolgmeting Bewustwordingsacties medewerkers Naleving beleid
Check	:	Interne controle Managementrapportages Kwetsbaarheden onderzoek Pentesten Social engineering (oa mistery guest)
Do	:	Evaluatie Verbetervoorstellen Implementatie verbeteringen

Terugkerend tijdschema

1. Beleidsvorming – het formuleren van het informatiebeveiligingsbeleid (dit document – 3 jaarlijks) vaststellen door het Dagelijks Bestuur
2. Risicoanalyse – onderzoek waar welke risico's bestaan (continue)
3. Informatiebeveiligingsplan (jaarlijks)
4. Controles (continu)
5. Evaluatie en controle (jaarlijks)
6. Implementatie – uitvoeren van de maatregelen uit het informatiebeveiligingsplan (continu)
7. Rapporteren bevindingen (jaarlijks); ter kennisname aan het Dagelijks Bestuur

3.1.1 Beleidsvorming

Het informatiebeveiligingsbeleid wordt opgesteld door de CISO en na bespreking in het Management Team ter vaststelling voorgelegd aan het dagelijks bestuur van de RBG.

De ontwikkelingen gaan snel waardoor ook de risico's steeds veranderen. Het beveiligingsbeleid dient daarop in te spelen en zal daarom minimaal 1 keer in de drie jaar worden geactualiseerd.

Het vastgestelde beleid wordt vervolgens kenbaar gemaakt aan alle medewerkers van de Regionale Belasting Groep.

3.1.2 Risicoanalyse

Jaarlijks voert de Regionale Belasting Groep een risicoanalyse uit over de gehele reikwijdte van de BIO (Baseline Informatiebeveiliging Overheid). Vervolgens wordt op basis van de inventarisatie een inschatting gemaakt van de kans en impact. Dit leidt op zijn beurt tot een risico kwalificatie:

- Maatregelen die de organisatie beschermen tegen hoge risico's krijgen prioriteit 1. Advies: **maatregel uit voeren**
- Maatregelen die de organisatie beschermen tegen middel grote risico's prioriteit 3. Advies: **overweeg deze maatregelen**
- Maatregelen die de organisatie beschermen tegen lage risico's krijgen prioriteit 5. Advies: **accepteer deze risico's**

Op basis van de uitkomsten van risicoanalyses en controles (oa nulmeting, IT audit, kwetsbaarhedenscan, pentest, social-engineering, etc) wordt een informatiebeveiligingsplan opgesteld. In dit plan wordt beschreven welke maatregelen worden genomen om de risico's weg te nemen of te beperken. In principe worden de risico's met prioriteit 1 als eerste opgepakt. Het uitvoeringsplan wordt vastgesteld door het Management.

3.1.3 Informatiebeveiligingsplan

Het uitvoeringsplan wordt vastgesteld door het Management Team.
De clustermanagers zijn verantwoordelijk voor de uitvoering en naleving van het beveiligingsplan. Desgewenst zullen zij coördinerende taken m.b.t. informatiebeveiliging toewijzen aan de medewerkers. Jaarlijks rapporteren de clustermanagers over de lijn en de CISO over de concern voortgang, van de implementatie van de voorgestelde maatregelen.

3.1.4 Controles en evaluatie

De controle op uitvoering van de vastgestelde beveiligingsmaatregelen wordt door de kwaliteitsmedewerkers uitgevoerd. De controles omvatten minimaal het volgende:

- Controle op naleving van het vastgestelde beleid en hieruit voortvloeiende richtlijnen en maatregelen;
- Controle op de implementatie en borging van maatregelen uit het beveiligingsplan;

Zij rapporteren hun bevindingen aan de lijn en de CISO. Deze zal deze rapportage(s) aanvullen en vervolgens met het Management Team bespreken.

De verantwoordelijkheid voor implementatie van de beveiligingsmaatregel ligt bij de clustermanagers. Zij dienen in hun reguliere PDCA-rapportages aandacht te besteden aan de voortgang van implementatie van maatregelen uit het beveiligingsplan.

3.1.5 Rapportage bevindingen

Jaarlijks wordt een rapportage gemaakt over eventuele beveiligingsincidenten en kwetsbaarheden en de hierop genomen maatregelen. Deze rapportage zal worden vastgesteld door het Management Team en ter kennisneming aan het Dagelijks bestuur worden aangeboden.

4. Eigenaarschap informatiesystemen

De RBG beschikt over zeer veel informatie die op verschillende manieren wordt opgeslagen en uitgewisseld (zowel digitaal als analoog). De RBG beschikt over een breed scala aan bedrijfsmiddelen die beheerd worden. Al deze bedrijfsmiddelen en informatie zijn blootgesteld aan risico's zoals diefstal, beschadiging of onoordeelkundig gebruik. Voor alle ICT-configuratie items is duidelijk wie de eigenaar/hoofdgebruiker is en wie verantwoordelijk is.

Eventuele onduidelijkheid over de vraag wie verantwoordelijk is voor gegevensbestanden heeft tot gevolg dat niemand zich verantwoordelijk voelt voor de beveiliging en niemand echt zal optreden bij incidenten.

Het team ICT, onderdeel van de staf, houdt in een configuratie management database (CMDB) een actuele registratie bij van bedrijfsmiddelen die voor de organisatie een belang vertegenwoordigen zoals informatie(verzamelingen), software, hardware en diensten. Tevens wordt vastgelegd met wie, welke en hoe vaak informatie wordt uitgewisseld.

De uitgangspunten voor het toekennen van autorisaties worden jaarlijks getoetst en vastgelegd. Het Management Team van de RBG bekrachtigt deze jaarlijks.

In de matrix staat de uitwerking hiervan per team/medewerker. De uitgangspunten en de matrix zijn in goed overleg tot stand gekomen tussen ICT en de diverse teams binnen de RBG.

In het jaarlijkse Informatiebeveiligingsplan wordt per informatiesysteem (hiermee bedoelen we niet de software) aandacht besteedt aan :

- Wie de eigenaar is van het informatiesysteem (proces)
- Wat de gegevensclassificatie is
- Wat het gewenste beveiligingsniveau van het systeem is

De eigenaar van een applicatie heeft de volgende verantwoordelijkheden:

- Bewaken beveiligingsmaatregelen die de beschikbaarheid, integriteit en vertrouwelijkheid beschermen.
- Bij onwenselijke problemen informeert de eigenaar direct de CISO
- Als hij afwijkt van het beveiligingsbeleid dan doet hij dat in samenspraak met de CISO. Deze zorgt voor een strikte onderbouwing en registratie van de afwijking.
- De eigenaar wordt bij wijzigingen aan het informatiesysteem altijd geïnformeerd. Wijzigingen mogen alleen met toestemming van de eigenaar worden aangebracht zodat hij de impact van de wijziging op de informatiebeveiliging kan beoordelen.

4.1 Classificatie van informatie en systemen
Om te kunnen bepalen welke beveiligingsmaatregelen moeten worden getroffen t.a.v. processen en informatiesystemen worden beveiligingsclassificaties gebruikt. Classificatie maakt het vereiste beschermingsniveau zichtbaar en maakt duidelijk welke maatregelen nodig zijn.

Er wordt geclassificeerd op drie betrouwbaarheidsaspecten van informatie (BIV):

- Beschikbaarheid
- Integriteit (juistheid, volledigheid en tijdigheid)
- Vertrouwelijkheid

Er zijn drie beschermingsniveaus van laag naar hoog. Daarnaast is er nog een niveau 'geen'. Dit niveau geeft aan dat er geen beschermingseisen worden gesteld, bijvoorbeeld omdat informatie openbaar is. De niveaus zijn in onderstaande tabel weergegeven.

Niveau	Beschikbaarheid	Integriteit	Vertrouwelijkheid
Geen	**Niet nodig** gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn *(bv: ondersteunende tools als routeplanner)*	**Niet zeker** informatie mag worden veranderd *(bv: templates en sjablonen)*	**Openbaar** informatie mag door iedereen worden ingezien *(bv: algemene informatie op de externe website van de RBG*
Laag	**Belangrijk** informatie mag incidenteel niet beschikbaar zijn *(bv: administratieve gegevens)*	**Beschermd** het bedrijfsproces staat enkele (integriteits-) fouten toe *(bv: rapportages)*	**Bedrijfsvertrouwelijk** informatie is toegankelijk voor alle medewerkers van de organisatie *(bv: informatie op het de G-schijf)*
Midden	**Noodzakelijk** informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk *(bv: primaire proces informatie)*	**Hoog** het bedrijfsproces staat zeer weinig fouten toe *(bv: bedrijfsvoeringinformatie en primaire procesinformatie)*	**Vertrouwelijk** informatie is alleen toegankelijk voor een beperkte groep gebruikers *(bv: persoonsgegevens, financiële gegevens)*
Hoog	**Essentieel** informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten *(bv: basisregistraties)*	**Absoluut** het bedrijfsproces staat geen fouten toe *(bv: op de digitale balie)*	**Geheim** informatie is alleen toegankelijk voor direct geadresseerde(n) *(bv strafrechtelijke informatie.)Voor de RBG is dit niet van toepassing.*

Het belang van informatie(systemen) voor de organisatie alsmede de privacy gevoeligheid van gegevens verschilt per systeem en gegeven. De Regionale Belasting Groep stelt normen op voor wat betreft Beschikbaarheid, Integriteit en Vertrouwelijkheid. Deze normen liggen voor de RBG vast in het *procesverbaal* ***"Gegevens classificatie"*** en worden na bespreking in het Management Team vastgesteld door de directeur.

5. Medewerkers

Beveiliging is zo sterk als de zwakste schakel. De praktijk leert dat dit bij informatiebeveiliging niet anders is. Bij informatiebeveiliging kunnen technische voorzieningen veel beschermen maar als medewerkers niet bewust zijn van informatiebeveiliging vormen zij de zwakste schakel.

5.1 Beveiligingseisen van personeel
Bij indiensttreding wordt de nodige aandacht geschonken aan privacy, integriteit en informatiebeveiliging.

Vast personeel

Personeel dat in dienst is bij de RBG valt onder de Wet Normalisering Rechtspositie Ambtenaren (WRNA) per 1 januari 2020. Naar aanleiding hiervan is het Personeelshandboek vastgesteld, waarvan onderstaande regelingen deel uitmaken:
- Gedragscode elektronisch verkeer
- Gedragscode gebruik van bedrijfsmiddelen

Dit betekent dat nieuwe medewerkers bij de aanstelling niet apart een verklaring hoeven te ondertekenen dat zij op verantwoorde wijze omgaan met privacygevoelige informatie. In de arbeidsovereenkomst (art. 11 Personeelshandboek) wordt hiernaar verwezen.
Voor wat betreft integriteit legt de ambtenaar een eed of belofte af.

Daar waar het gaat om informatiebeveiliging wordt de medewerker regelmatig geattendeerd op het belang hiervan. In het opleidingsprogramma is informatiebeveiliging één van de aandachtspunten.

Tijdelijk personeel

Tijdelijk personeel is personeel dat werkzaamheden verricht bij de RBG en niet valt onder de WRNA. Zij zijn gedetacheerd via een uitzendbureau of op andere wijze ingehuurd. Deze tijdelijke medewerkers tekenen op de eerste werkdag bij de RBG een *verklaring*, dat volgens de gestelde eisen omgegaan wordt met privacygevoelige informatie, gedragsregels internetgebruik etc. Ook tekenen deze medewerkers een *geheimhoudingsverklaring*.

Werkwijze

Bij indiensttreding (zowel vast als tijdelijk personeel) wordt gebruikgemaakt van een standaard werkwijze.

- De clustermanager is verantwoordelijk voor het juist afhandelen van de beveiligingsaspecten van het aangaan, wijzigen en beëindigen van een dienstverband of een overeenkomst met externen.
- Bij beëindiging van het dienstverband en inhuur worden alle bedrijfsmiddelen van de organisatie geretourneerd. Autorisaties worden in opdracht van de proceseigenaar van het desbetreffende bedrijfsproces ingetrokken.
- Voor vaste medewerkers die werken met vertrouwelijke of geheime informatie wordt gevraagd voor indiensttreding een Verklaring Omtrent het Gedrag (= VOG) te laten overleggen. De VOG wordt indien nodig herhaald tijdens het dienstverband.
- Tijdelijk personeel moet een geheimhoudingsverklaring ondertekenen
- De eigenaar van het bedrijfsproces bepaalt welke rol(len) de medewerker moet vervullen en welke autorisaties voor het raadplegen, opvoeren, muteren en afvoeren van gegevens moeten worden toegepast.
- Bij inbreuk op de beveiliging gelden voor medewerkers disciplinaire maatregelen, zoals onder meer genoemd in de WNRA en andere regelingen.
- Regels die volgen uit dit beleid en andere regelingen gelden ook voor externen, die in opdracht van de RBG werkzaamheden uitvoeren.

5.2 Opleidingen
Alle medewerkers (en voor zover van toepassing externe gebruikers van onze systemen) worden getraind in de geldende procedures voor informatiebeveiliging. Deze trainingen worden regelmatig herhaald om het beveiligingsbewustzijn op peil te houden.

Naast de opleiding zullen de medewerkers ook via interne campagnes bewust gemaakt worden van het belang van informatiebeveiliging en privacy. Dit alles heeft een terugkerend karakter.

5.3 Beveiligingsincidenten
Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de, beschikbaarheid, integriteit of vertrouwelijkheid van informatie of informatie systemen in gevaar is of kan komen. Bij beveiligingsincidenten wordt de CISO altijd geïnformeerd.

Alle beveiligingsincidenten en datalekken worden geregistreerd. Ook de genomen maatregelen om de impact van het incident te beperken of weg te nemen worden vastgelegd. Deze informatie wordt later gebruikt ter evaluatie van het incident. Het verzamelen van deze informatie heeft ook als doel de beheersmaatregelen te verbeteren.

Voor het melden van een datalek heeft de RBG een *Protocol melding aan Autoriteit Persoonsgegevens* opgesteld.

6. Beveiliging

De RBG is volledig afhankelijk van IT-voorzieningen voor het verrichten van de primaire en secundaire processen. Uitval van deze voorzieningen heeft tot gevolg dat nagenoeg alle bedrijfsprocessen stil vallen. Het beheer van ICT-voorzieningen is door de RBG uitbesteed aan derde partijen. De eisen met betrekking tot beschikbaarheid, datarecovery, beveiliging etc. zijn contractueel vastgelegd.

Het gehele werkproces, primair en secundair, is ondergebracht bij derden partijen als een service en derhalve maakt de RBG zelf geen gebruik van fysieke gegevensdragers. Aan de medewerkers zijn laptops beschikbaar gesteld om zijn of haar werkzaamheden uit te voeren. Naast het gebruik van de laptops is er de mogelijkheid om via een beveiligde verbinding met authenticatie te werken vanaf alle apparatuur met een internetverbinding.

Met betrekking tot beveiliging van de fysieke ruimte, het gebruik van apparatuur, gebruik van gegevens dragers, back-up en recovery, stroomvoorziening, clean desk en clean screen, reparatie apparatuur etc. zijn door de RBG normen vastgesteld.

6.1 Beveiliging van apparatuur

Door de moderne manier van werken binnen de RBG zijn bedrijfsgegevens alleen nog via een beveiligde manier te raadplegen of te bewerken. Doormiddel van een Multi Factor Authenticatie (MFA) krijgen medewerkers toegang tot de beveiligde omgeving.

Zowel zakelijk als privé kunnen medewerkers gebruik maken van een door de RBG uitgegeven en beheerde laptop. Deze kan alleen door MFA worden geopend. Hierbij wordt gebruik gemaakt van zowel biometrisch als niet-bio metrische beveiligingen.

Daarnaast kunnen medewerkers via een eigen mobiel telefoon en tablet toegang krijgen tot het systeem. Dit kan alleen via MFA. De gegevens staan en blijven ten alle tijden in een beveiligde cloud omgeving. De mogelijkheid om gegevens lokaal te bewaren zijn alleen mogelijk in een afgeschermde en versleutelde omgeving (OneDrive).

Indien een apparaat fysiek zoekraakt of gestolen wordt, blijft de data van de Regionale Belasting Groep versleuteld en is niet toegankelijk voor derden.

6.2 Stroom voorziening

De Regionale Belasting Groep maakt gebruik van kantoorruimte in een bedrijfsverzamelgebouw in Schiedam. Dit pand wordt gedeeld met andere huurders. In het pand is een noodstroomvoorziening aanwezig die het gehele pand (dus alle huurders) ingeval van stroomuitval van stroom moet voorzien. De stroomvoorziening in Nederland is dermate betrouwbaar dat de Regionale Belasting Groep geen noodzaak ziet om verder maatregelen tegen stroomuitval te nemen

6.3 Gebruik USB-poorten

Het zelfstandig kopiëren van gegevens naar randapparatuur (zoals een usb-stick) is niet toegestaan en het benaderen van de USB-poorten op de laptops is uitgeschakeld. Tevens wordt het kopiëren van data van bijvoorbeeld een telewerkplek naar het netwerk van de RBG afgesloten.

6.4 Wachtwoorden

Wachtwoorden vormen een belangrijk aspect van de informatiebeveiliging. Wachtwoorden zorgen ervoor dat onbevoegden minder makkelijk toegang kunnen krijgen tot informatie. Een gemakkelijk wachtwoord evenals onduidelijke of niet gevolgde wachtwoord procedures zijn een bedreiging voor de vertrouwelijkheid en integriteit van informatie. Alle gebruikers dienen goede (sterke) wachtwoorden te kiezen en zijn verantwoordelijk voor de geheimhouding van hun wachtwoorden en login-gegevens.

Wanneer gewerkt wordt met de systemen van de Regionale Belasting Groep op een andere locatie dan het kantoorpand in Schiedam, dient bij het inloggen, naast de gebruikersnaam en wachtwoord, een tweede beveiliging, een Authenticator, te worden gebruikt (Multi Factor Authenticatie).

6.5 Verantwoordelijkheden t.a.v. beheer netwerken

Het beheer van het netwerk is door de Regionale Belasting Groep uitbesteed aan KPN Modern Work Place (MWP). Zij zijn primair verantwoordelijk voor het beheer van het netwerk.

Daar waar de RBG derden toegang geeft tot zijn netwerk (denk aan ondersteunende bedrijven, deelnemers aan de gemeenschappelijke regeling van de RBG etc.) wordt gebruikgemaakt van beveiligde netwerkverbindingen (VPN, huurlijnen etc.).

6.5.1 Gebruik van internetfaciliteiten

Via het netwerk van de Regionale Belasting Groep is het toegestaan om van e-mail en internet gebruik te maken. De voorwaarden waaronder dit is toegestaan zijn vastgelegd in de *Uitvoeringsregeling gedragscode elektronisch verkeer*.

In het Service Level Agreement met KPN Modern Work Place is vastgelegd dat toegang tot het fysieke netwerk op locatie Scheidam beveiligd is met een zogenaamde firewall.

6.5.2 Verplichte netwerkroute

Alle datatransport vindt plaats door middel van vaste bekabeling die gecontroleerd is op betrouwbaarheid. Op dit netwerk vindt actieve monitoring plaats door de netwerkbeheerders.

Binnen de RBG wordt gebruik gemaakt van een eigen netwerk (LAN) dat middels externe netwerken (WAN) is verbonden met de leverancier van de hosting KPN MWP , Microsoft Azure en Centric in Amsterdam. Ten behoeve van specifieke taken is het LAN verbonden met het internet. Ook deze verbinding is voorzien van een firewall. Het datanetwerk is getoetst aan vastgestelde normen.

6.5.3 Netwerktoegang

Alle op het netwerk aangesloten werkstations/laptops worden bij aanmelding geïdentificeerd door de server. Bij gebruikmaking van ons interne netwerk kan een medewerker na het invoeren van zijn gebruikersnaam, wachtwoord en of biometrische gegevens gebruik maken van het netwerk. Bij meer dan drie foutieve aanmeldpogingen wordt het gebruikersnaam van de medewerker geblokkeerd. Via de applicatiebeheerders kan dit weer worden vrijgegeven.

6.5.4 Beveiliging netwerken

Alle transport van data via openbare netwerken dient beveiligd plaats te vinden. Daar waar mogelijk wordt gebruikgemaakt van encryptie (versleuteling). Voor het verzenden van bestanden door individuele medewerkers worden faciliteiten beschikbaar gesteld om dit op een eenvoudige maar veilige manier te kunnen doen.

Voor netwerken die gebruikt worden voor het ontsluiten van de landelijke informatiesystemen (landelijkvoorzieningen) worden van extra beveiligingsmaatregelen genomen. Beveiliging van deze netwerken dient van het hoogste niveau te zijn.

7. Beheer van communicatie en bedieningsprocessen

Het is van groot belang dat onze systemen op een juiste manier worden gebruikt. Naast opleidingen en werkinstructies is de nodige documentatie beschikbaar in de kennisbank. Het ontbreken van documentatie kan leiden tot fouten, niet-uniforme wijze van gegevensinvoer of in geval de beheerder/bediener uitvalt tot problemen rondom de continuïteit.

Ook onjuiste autorisaties kunnen leiden tot foutieve handelingen, fraude en verduistering. Daarom dient er een actuele autorisatiesmatrix aanwezig te zijn. Deze wordt minimaal één keer per jaar gecontroleerd. In beginsel mag niemand autorisaties hebben om een gehele cyclus van handelingen in een informatiesysteem te beheersen, zodanig dat beschikbaarheid, integriteit of vertrouwelijkheid kan worden gecompromitteerd. Indien dit toch noodzakelijk is, dient een audit trail te worden vastgelegd van alle handelingen en tijdstippen in het proces, dusdanig dat transactie kan worden herleid. De audit trail is niet toegankelijk voor degene wiens handelingen worden vastgelegd.

De RBG gaat steeds meer samenwerken (en informatie uitwisselen) in ketens en besteedt veel taken uit. Bij beheer van systemen en gegevens door een derde partij kan ook informatie van de RBG op straat komen te liggen. De RBG blijft verantwoordelijk voor de informatiebeveiliging van haar gegevens in dat deel van de keten waarbij het beheer bij een andere partij ligt. In de contracten met derde partijen is altijd een paragraaf opgenomen met betrekking tot beveiliging. In het kader van de AVG worden verwerkersovereenkomsten afgesloten met deze partijen.

Bij externe hosting van data en/of services (uitbesteding, SaaS) blijft de RBG eindverantwoordelijk voor de betrouwbaarheid van de uitbestede diensten. Dit is gebonden aan regels en vereist verwerkingsovereenkomsten en een controle hierop.

7.1 Bring Your Own Device (BYOD)

De Regionale Belasting Groep staat het gebruik van privéapparatuur (devices) toe voor zakelijk gebruik :

- Mobiele telefoon
- Smartphone
- Tablet
- Laptop
- PC

Doordat de RBG al haar processen en gegevens heeft onder gebracht in een SaaS (Software as a Service), is het voor medewerkers en externe medewerkers mogelijk om vanaf eigen apparatuur via Multi Factor Authenticatie (MFA) toegang te krijgen tot de beveiligde omgeving werkomgeving. De beveiliging van de systemen laat het niet toe om gegevens lokaal op te slaan of op een andere gegevensdrager.
Door de toegepaste beveiligingsmaatregelen worden er geen verplichte randvoorwaarden gesteld aan externe apparatuur. Voor thuiswerken wordt wel een stabiele verbinding vereist.

7.2 Veilig afvoeren en hergebruiken van apparatuur

De RBG heeft laptops voor haar medewerkers uitgereikt, hiervoor is een bruikleenovereenkomst opgesteld.

Door de ver-SaaS-ing en beveiligingsmaatregelen van de werkzaamheden is het niet mogelijke om gegevens op externe gegevensdragers op te slaan. Alleen voor back-up doeleinde wordt gebruik gemaakt van externe harde schijven, deze bevinden zich in een fysieke kluis. Alleen medewerkers van ICT hebben toegang tot deze kluis.

Als laptops worden vervangen of geretourneerd dienen de gegevens en software van deze apparaten te worden verwijderd. De RBG volgt hier een protocol.

8. Responsible disclosure

Kwetsbaarheden in ICT kunnen op diverse plaatsen in hard- en software voorkomen en kennen vele gradaties. Gemeenschappelijke deler is dat het misbruik van de kwetsbaarheid kan leiden tot mogelijke veiligheidsrisico's.

Systemen kunnen door kwetsbaarheden mogelijkerwijs uitvallen (beschikbaarheid), data binnen het systeem kunnen gewijzigd worden (integriteit) en data kunnen toegankelijk worden voor personen die daar niet toe gemachtigd zijn (vertrouwelijkheid).

ICT-kwetsbaarheden kunnen voor de RBG ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid grote gevolgen hebben.

Een klant kan door gebruik te maken van diensten van de RBG bedoeld of onbedoeld tegen, voor de RBG onbekende, kwetsbaarheden stuiten. In zo'n geval wil de RBG graag tijdig geïnformeerd worden, zodat passende maatregelen genomen kunnen worden om de kwetsbaarheid weg te nemen.

De responsible disclosure kan bijdragen aan de veiligheid van ICT systemen en het beheersen van de kwetsbaarheid van ICT-systemen door kwetsbaarheden op verantwoorde wijze te melden zodat schade zo veel als mogelijk kan worden voorkomen of beperkt. Bij de responsible disclosure staat voorop dat partijen zich over en weer houden aan afspraken over het melden van de kwetsbaarheid en de omgang hiermee.

Door het opstellen van een responsible disclosure maakt de RBG duidelijk op welke wijze zij wil omgaan met meldingen van kwetsbaarheden.

- De RBG maakt het beleid voor responsible disclosure publiekelijk kenbaar.
- De RBG maakt het laagdrempelig voor een melder om een melding te doen. Dit kan bijvoorbeeld een online formulier, te gebruiken voor het doen van meldingen.
- Meldingen over een kwetsbaarheid worden direct naar het team ICT verzonden zodat deze de melding kan beoordelen en in behandeling kan nemen.
- De RBG stuurt een ontvangstbevestiging van de melding aan de melder. Hierna treden de organisatie en de melder in contact over het verdere proces.
- De RBG bepaalt in overleg met de melder de termijn waarop eventuele bekendmaking zal plaatsvinden.

- De RBG houdt de melder en overige betrokkenen op de hoogte van de voortgang van het proces.
- De RBG kan in overleg met de melder afspreken om de bredere ICT-community te informeren over de kwetsbaarheid indien het aannemelijk is dat de kwetsbaarheid ook op andere plaatsen aanwezig is.
- De RBG zal geen juridische stappen ondernemen indien conform het beleid wordt gehandeld.

9. Vaststelling

Vastgesteld in de vergadering van het dagelijks bestuur van de Regionale Belasting Groep van 19 april 2023.

Het dagelijks bestuur van de Regionale Belasting Groep,

directeur,
H.B. Sigmond

voorzitter,
drs. A.J.B. van der Klugt