REGIONALE BELASTING GROEP

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 222

13 maart 2020

Officiële uitgave van de gemeenschappelijke regeling Regionale Belasting Groep

Besluit van het dagelijks bestuur van de gemeenschappelijke regeling Regionale Belasting Groep houdende regels omtrent informatiebeveiliging

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). Steeds meer informatie is digitaal beschikbaar en wordt digitaal uitgewisseld. Opslag van gegevens is niet zelden in de cloud. Tablets met verbindingen naar bedrijfsnetwerken zijn geen uitzondering. Mobiele telefoons zijn zeer krachtige computers geworden waarmee eenvoudig en snel informatie uitgewisseld kan worden. De Regionale Belasting Groep heeft met al deze ontwikkelingen te maken.
De afgelopen jaren neemt het aantal incidenten rondom informatiebeveiliging toe. Recent hebben we wereldwijde cyberaanvallen met ransomware gezien. Overheden, banken, havenbedrijven en andere grote organisaties zijn getroffen door deze aanvallen. De financiële gevolgen van dergelijke aanvallen zijn enorm. Deze 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. Zonder de gegevens en/of systemen zou onze organisatie niet kunnen werken.
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. Het bekendste voorbeeld hiervan zijn de Wet Bescherming Persoonsgegevens (WBP) en de Algemene verordening gegevensbescherming (AVG).

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 de beveiliging van niet digitale gegevensdragers en de fysieke beveiliging van ons gebouw en medewerkers.

1.2.1 Geformuleerde kaders

1. Informatiebeveiliging is geen apart technisch onderwerp. Het belang van informatiebeveiliging zal bij alle medewerkers (en managers) bekend moeten zijn.
2. Bewustwording en opleiding. Binnen de opleidingen van de RBG-academie zal de nodige aandacht besteed worden 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 Gemeenten (BIG).
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 manager informatiebeveiliging ondersteunt hierbij;
6. Informatiebeveiliging draagt bij aan het operationeel houden van de bedrijfsprocessen. Het is geen doel op zich en mag de bedrijfsprocessen niet verstoren.
7. Alle processen en informatiesystemen (zowel digitaal als analoog) hebben een formele eigenaar binnen de organisatie.
8. Maatregelen zijn in balans met de te beschermen waarde;
9. Alle noodzakelijke maatregelen worden genomen om te voldoen aan wet- en regelgeving op het gebied van informatiebeveiliging.
10. Daar waar afgeweken wordt van vastgesteld beleid of standaarden, legt het management dit vast in een formele verklaring.
11. Een medewerker beschikt over de informatie die hij voor zijn functie nodig heeft. Door middel van gebruikersnaam en wachtwoord wordt binnen de informatiesystemen functiescheiding toegepast.

1.3 Scope
Informatiebeveiliging is meer dan ICT, computers en automatisering. 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) en alle informatie verwerkende systemen (applicaties, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen), maar vooral ook over mensen en processen. Studies laten zien dat de meeste incidenten niet voortkomen uit gebrekkige techniek, maar vooral door menselijk handelen en een tekortschietende 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, de programmatuur en alle informatie/gegevens die de Regionale Belasting Groep gebruikt.

2. Organisatie van informatiebeveiliging en privacy
Het bestuur en het 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 hebben, de risico's die de RBG hiermee loopt en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan zet het management dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.
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 een informatiebeveiligingsbeleid van en voor de hele de RBG. Dit 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 Nederlandse Gemeenten (BIG).
- De RBG stelt dit normenkader vast, waarbij er ruimte is voor afweging en prioritering op basis van het 'pas toe of leg uit' principe.

2.1 Verantwoordelijke functionarissen
Periodiek wordt in het managementoverleg informatiebeveiliging en informatiebeheer besproken. De clustermanagers zijn verantwoordelijk voor de handhaving van het beleid.

2.1.1 CISO
Functioneel is de Controller benoemd als Corporate Information Security Officer (CISO). In dit beleidsdocument wordt deze functie aangeduid als manager Informatiebeveiliging. In deze hoedanigheid ondersteunt hij de clustermanagers.
De manager Informatiebeveiliging rapporteert rechtstreeks aan de directeur. De manager Informatiebeveiliging 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.
Wanneer, als gevolg van een beveiligingsincident contact wordt opgenomen met autoriteiten (InformatieBeveiligingsDienst (IBD) of Autoriteit Persoonsgegevens(AP)), is de manager Informatiebeveiliging verantwoordelijk voor dergelijke contacten.

2.2 Privacybescherming
Naast informatiebeveiliging is ook privacybescherming van groot belang. De Wet bescherming persoonsgegevens biedt organisaties ruimte om een Privacy Officer (PO) en Functionaris Gegevensbescherming (FG) aan te stellen.

2.2.2 Functionaris Gegevensbescherming
Vanuit de huidige privacywetgeving (Wbp) is het voor organisaties optioneel een Functionaris Gegevensbescherming (FG) aan de stellen. Onder de komende Europese privacyverordening (AVG), die in mei 2018 van kracht wordt, 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.

2.2.3 Privacy Officer
Waar de CISO verantwoordelijk is voor het informatiebeveiligingsbeleid is de Privacy Officer(PO) verantwoordelijk voor het vormgeven en bewaken van het privacybeleid binnen de organisatie. Daarnaast kan de PO ondersteunen bij het in kaart brengen van de risico's door bijvoorbeeld een Privacy Impact Assessment (PIA) uit te voeren. Een PIA 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 vakafdelingen 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?
Uit bovenstaande kan opgemaakt worden dat in kader van functiescheiding de PO niet tevens FG kan zijn.

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 primair de verantwoordelijkheid van de clustermanagers.

Doelgroep	**Relevantie voor Informatiebeveiligingsbeleid**
Dagelijks Bestuur	Integrale verantwoordelijkheid
Directie	Kaderstelling en implementatie
Clustermanagers	Sturing op informatieveiligheid en controle op naleving
Alle medewerkers	Gedrag en naleving
Proces en gegevenseigenaren	Classificatie: bepalen van beschermingseisen van informatie
het management team	Planvorming binnen de informatiebeveiligingskaders
Manager Informatiebeveiliging	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	Onafhankelijke toetsing van het beleid
Leveranciers en ketenpartners	Compliance aan het beleid

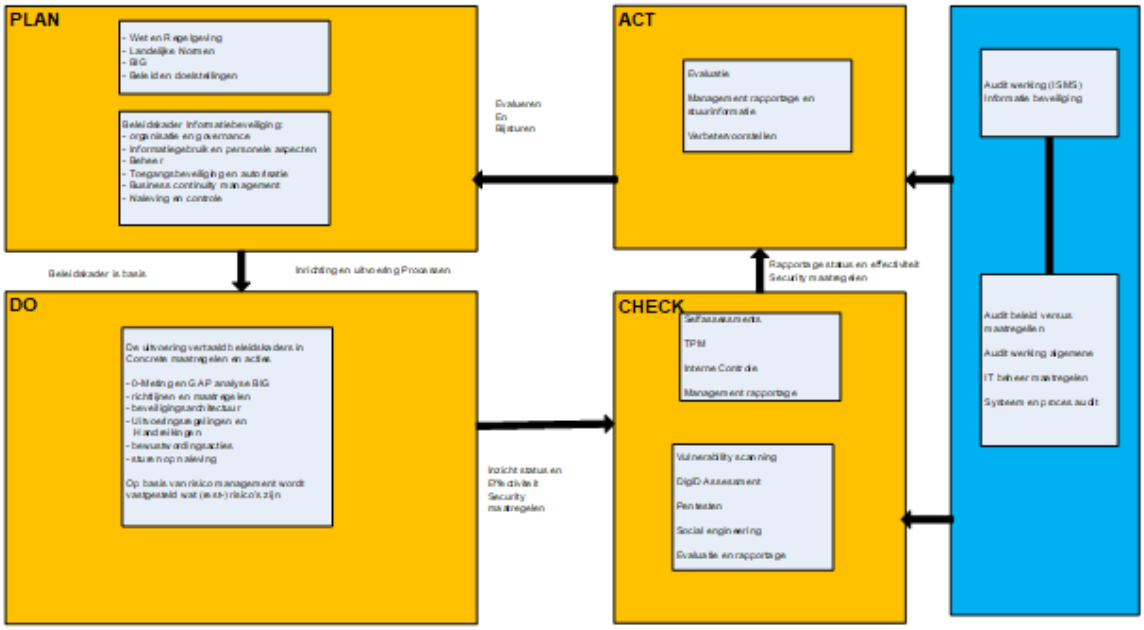
Visie

De komende jaren zet de RBG 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, maar is tegelijkertijd een 'enabler'; het maakt bijvoorbeeld elektronische dienstverlening op verantwoorde wijze mogelijk, evenals nieuwe, 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 medewerkers is essentieel voor informatieveiligheid. Informatiebeveiliging dient een integraal onderdeel van de reguliere werkwijze te zijn. Informatiebeveiligingsaspecten worden derhalve in alle procesbeschrijvingen en werkinstructies opgenomen. Naast de procesbeschrijvingen en instructies wordt ook in afdelingsplannen aangegeven welke maatregelen zijn genomen om informatiebeveiliging te waarborgen.

3.1 Beleidsproces
Het proces om beveiligingsbeleid vast te stellen en hier uitvoering aan te geven, verloopt als volgt:
1. Beleidsvorming – het formuleren van het informatiebeveiligingsbeleid (dit document).
2. Jaarlijkse risicoanalyse – onderzoek waar welke risico's bestaan.

3. Planvorming – opstellen informatiebeveiligingsplan. Het streven is om dit plan voor eind 2018 gereed te hebben.
4. Implementatie – uitvoeren van de maatregelen uit het informatiebeveiligingsplan
5. Evaluatie en controle – onderdeel van de PDCA-cyclus.



Information Security Management System

3.1.1 Beleidsvorming

Het informatiebeveiligingsbeleid wordt door de manager Informatiebeveiliging uitgewerkt en 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 periodiek geactualiseerd worden.
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 BIG (Baseline Informatiebeveiliging Gemeenten). 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 2. Advies: overweeg deze maatregelen
- Maatregelen die de organisatie beschermen tegen lage risico's krijgen prioriteit 3. Advies: accepteer deze risico's

Op basis van de uitkomsten van de risicoanalyse wordt een informatiebeveiligingsplan opgesteld. In dit plan is 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. Wanneer er zwaarwegende redenen zijn kan ook een knelpunt met lagere prioriteit met voorrang worden opgepakt. Het uitvoeringsplan wordt vastgesteld door het de directeur en zal ter kennisneming aan de dagelijks bestuur worden toegezonden.

3.1.4 Implementatie

De clustermanagers zijn verantwoordelijk voor de uitvoering van de maatregelen. In de verschillende afdelingsplannen geven zij aan hoe en wanneer de maatregelen uit het beveiligingsplan worden uitgevoerd. Desgewenst kunnen zij coördinerende taken m.b.t. informatiebeveiliging toewijzen aan de medewerkers.

3.1.5 Evaluatie en controle

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 manager Informatiebeveiliging. De manager Informatiebeveiliging zal deze rapportage(s) aanvullen en vervolgens met de directeur en de clustermanagers bespreken.
De verantwoordelijkheid voor implementatie van beveiligingsmaartregelen ligt bij de clustermanagers. Zij dienen in hun reguliere PDCA-rapportages aandacht te besteden aan de voortgang van implementatie van maatregelen uit het beveiligingsplan.

4. Eigenaarschap informatiesystemen

De RBG beschikt over zeer veel informatie die op verschillende manieren is opgeslagen en op verschillende manieren wordt 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, waarbij niet voor alle ICT-configuratie items duidelijk is wie de eigenaar/hoofdgebruiker is en wie verantwoordelijk is. 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 informatie hoe vaak wordt uitgewisseld. Van deze systemen etc. wordt vastgelegd:
- 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 manager informatiebeveiliging
- Als hij afwijkt van het beveiligingsbeleid dan doet hij dat in samenspraak met de manager Informatiebeveiliging. Hij zorgt in zo'n geval 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(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: Beschikbaarheid, Integriteit (juistheid, volledigheid en tijdigheid) en Vertrouwelijkheid (= BIV).

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	Vertrouwelijkheid	Integriteit	Beschikbaarheid
Geen	**Openbaar** informatie mag door iedereen worden ingezien *(bv: algemene informatie op de externe website van de RBG*	**Niet zeker** informatie mag worden veranderd *(bv: templates en sjablonen)*	**Niet nodig** gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn *(bv: ondersteunende tools als routeplanner)*
Laag	**Bedrijfsvertrouwelijk** informatie is toegankelijk voor alle medewerkers van de organisatie *(bv: informatie op het de G-schijf)*	**Beschermd** het bedrijfsproces staat enkele (integriteits-) fouten toe *(bv: rapportages)*	**Belangrijk** informatie mag incidenteel niet beschikbaar zijn *(bv: administratieve gegevens)*

Midden	**Vertrouwelijk** informatie is alleen toegankelijk voor een beperkte groep gebruikers *(bv: persoonsgegevens, financiële gegevens)*	**Hoog** het bedrijfsproces staat zeer weinig fouten toe *(bv: bedrijfsvoeringinformatie en primaire procesinformatie)*	**Noodzakelijk** informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk *(bv: primaire proces informatie)*
Hoog	**Geheim** informatie is alleen toegankelijk voor direct geadresseerde(n) *(bv strafrechtelijke informatie.)Voor de RBG is dit niet van toepassing.*	**Absoluut** het bedrijfsproces staat geen fouten toe *(bv: op de digitale balie)*	**Essentieel** informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten *(bv: basisregistraties)*

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 proces-verbaal "Gegevens classificatie" en worden 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 zich niet bewust zijn van informatiebeveiliging, dan vormen zij de zwakste schakel.

5.1 Beveiligingseisen bij aanname 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 direct onder het ambtenarenreglement. Dit betekent dat zij bij benoeming niet apart een verklaring hoeven te ondertekenen dat zij op verantwoorde wijze omgaan met privacygevoelige informatie. In het ambtenarenreglement is dit reeds opgenomen. 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 en in het opleidingsprogramma voor medewerkers is informatiebeveiliging één van de aandachtspunten.

Tijdelijk personeel

Tijdelijk personeel is personeel dat werkzaamheden verricht bij de RBG en niet in een ambtelijk dienstverband is benoemd, is gedetacheerd via een uitzendbureau of op andere wijze is 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.
Bij indiensttreding (zowel vast als tijdelijk personeel) wordt gebruikgemaakt van een standaard werkwijze.

- Het managementteam is verantwoordelijk voor het juist afhandelen van de beveiligingsaspecten van het aangaan, wijzigen en beëindigen van een dienstverband of een overeenkomst met externen. De HR-medewerker houdt toezicht op dit proces.
- Bij beëindiging van het dienstverband en de inhuur worden alle bedrijfsmiddelen van de organisatie geretourneerd. Autorisaties worden in opdracht van de proceseigenaar van het desbetreffende bedrijfsproces ingetrokken.
- Er wordt naar gestreefd om medewerkers die werken met vertrouwelijke of geheime informatie voor indiensttreding een Verklaring Omtrent het Gedrag (= VOG) te laten overleggen. De VOG wordt indien nodig herhaald tijdens het dienstverband.
- Ook bij inhuur wordt verzocht een Verklaring Omtrent het Gedrag (= VOG) te overleggen en wordt een geheimhoudingsverklaring getekend.
- 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 verstrekt.
- Bij inbreuk op de beveiliging gelden voor medewerkers disciplinaire maatregelen, zoals onder meer genoemd in het Ambtenarenreglement en andere regelingen.
- Regels die volgen uit dit beleid en andere regelingen gelden ook voor externen, die in opdracht van de belastingsamenwerking werkzaamheden uitvoeren.

5.2 Opleidingen

Alle medewerkers (en voor zover van toepassing externe gebruikers van onze systemen) dienen training te krijgen in de geldende procedures voor informatiebeveiliging. Deze training dient regelmatig te worden 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 manager informatiebeveiliging 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 opgesteld (Protocol meldingen aan Autoriteit Persoonsgegevens).

6. Fysieke beveiliging en beveiliging

De RBG is zeer afhankelijk van IT-voorzieningen voor het verrichten van de primaire 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.
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. De clustermanager ziet toe op handhaving van de beschreven procedures en normen.

6.1 Beveiliging van apparatuur

Er is een toename van het gebruik van mobiele gegevensdragers zoals smartphones, tablets en laptops. Het inzetten van mobiele apparaten zoals laptop, tablet of smartphone neemt nog steeds toe. Zowel zakelijk als privé maken medewerkers gebruik van dergelijke apparatuur. Ongeacht of het een zakelijk mobiel device is of een eigen mobiel device, immers op mobiele apparaten kan in meer of mindere mate data van de Regionale Belasting Groep staan. Los van het feit of het mobiele apparaat fysiek kan zoekraken, de data is in beide gevallen van de Regionale Belasting Groep. Beveiliging van de gegevens is vereist.

6.2 Stroom voorziening

De stroomvoorziening in Nederland is dermate betrouwbaar dat de Regionale Belasting Groep geen noodzaak ziet om maatregelen tegen stroomuitval te nemen.

6.3 Gebruik USB-poorten

Het zelfstandig kopiëren van gegevens naar randapparatuur (zoals een usb-stick) is niet toegestaan. Daarom is het gebruik van de USB-poorten op apparatuur van de Regionale Belasting Groep welke is aangesloten op het netwerk niet toegestaan. Het benaderen van de USB-poorten wordt beperkt.

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 wachtwoordprocedures zijn niet alleen een bedreiging voor de vertrouwelijkheid en integriteit van informatie, maar uiteindelijk ook slecht voor het imago van de Regionale Belasting Groep. Alle gebruikers dienen goede (sterke) wachtwoorden te kiezen en zijn verantwoordelijk voor de geheimhouding van hun wachtwoorden en login-gegevens.

7. Beheer van communicatie en bedieningsprocessen

Het is van groot belang dat onze systemen op een juiste manier worden gebruikt. Naast opleidingen en instructies is de nodige documentatie beschikbaar. 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 autorisatiematrix 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.

Er is een scheiding tussen beheertaken en overige gebruikstaken. Beheerwerkzaamheden worden alleen uitgevoerd wanneer is ingelogd als beheerder, normale gebruikstaken alleen wanneer is ingelogd als gebruiker.
De RBG gaat steeds meer samenwerken (en informatie uitwisselen) in ketens en besteedt meer 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 wordt 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, cloud computing) blijft de belastingsamenwerking eindverantwoordelijk voor de betrouwbaarheid van de uitbestede diensten. Dit is gebonden aan regels en vereist goede (contractuele) afspraken en controle hierop.

7.1 Bring Your Own Device (BYOD)

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

- Mobiele telefoon
- Smartphone
- Tablet
- Laptop

Zakelijk gebruik van bovengenoemde apparatuur is slechts toegestaan indien deze voldoet aan de door de Regionale Belasting Groep vastgestelde beveiligingseisen zoals vastgelegd in de BYOD-overeenkomst.

7.2 Stroomvoorziening

De stroomvoorziening in Nederland is dermate betrouwbaar dat de Regionale Belasting Groep geen noodzaak ziet om maatregelen tegen stroomuitval te nemen.

7.3 Veilig afvoeren en hergebruiken van apparatuur

Apparatuur en gegevensdragers kunnen vertrouwelijke gegevens bevatten die organisatie niet mogen verlaten. Gegevens kunnen zich bevinden in:

- laptops en desktop computers
- mobiele apparaten zoals smartphones en tablets
- printers
- scanners
- faxapparaten
- servers
- in draagbare media (geheugenkaarten, USB-sticks)

Als apparatuur wordt vervangen, dienen de gegevens van deze apparaten verwijderd te worden. De RBG stelt hiervoor een protocol op.

8. Responsible disclosure

Kwetsbaarheden in ICT komen op diverse plaatsen in hard- en software voor en kennen vele gradaties. Gemeenschappelijke deler is dat het uitbuiten 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, die in sterke mate afhankelijk is van ICT, 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 op, 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.
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 en deze meldingen zorgvuldig af te handelen, zodat schade zo veel als mogelijk kan worden voorkomen of beperkt. Bij 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 eigen beleid voor responsible disclosure maakt de RBG duidelijk op welke wijze zij wil omgaan met meldingen van kwetsbaarheden. Dit kan als volgt werken:

- 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 met 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. Een redelijke standaardtermijn die kan worden gehanteerd voor kwetsbaarheden in software is 60 dagen. Het verhelpen van kwetsbaarheden in hardware is lastiger te realiseren, hierbij kan een redelijke standaardtermijn van 6 maanden worden gehanteerd.
- 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.

10. Vaststelling

Vastgesteld in de vergadering van het dagelijks bestuur van de Regionale Belasting Groep op 26 april 2018.

Het dagelijks bestuur van de Regionale Belasting Groep,

directeur,

H.B. Sigmond

voorzitter,

drs. A.J.B. van der Klugt