SVB Gedragscode en regels voor integriteit

9357NX/0718

SVB
voor het leven
Sociale Verzekeringsbank

Inhoudsopgave

Inleiding

De SVB wil een prettige en stimulerende werkomgeving bieden. Om dit te kunnen garanderen hebben we een aantal regels opgesteld. De Gedragscode die deze lijnen beschrijft, is te zien als een overzicht van afspraken die we maken om verantwoord, vertrouwelijk, transparant en zorgvuldig met elkaar en onze werkzaamheden om te gaan. Deze gedragscode is een geactualiseerde versie van de SVB Gedragscode uit 2014.
Deze regels zijn "voor het geval dat", want wie altijd zorgvuldig en transparant handelt, zal zich vanzelfsprekend al aan de Gedragscode houden. Met 'integer gedrag' wordt doorgaans 'onkreukbaar', of 'rechtschapen' gedrag bedoeld.
Voor de SVB met haar maatschappelijke verantwoordelijkheid is het ook extra (gezichts)bepalend. Burgers moeten op de SVB en haar medewerkers kunnen vertrouwen.
Maar hoe bepaal je wat integriteit nu concreet voor de SVB betekent? Niet integer handelen, schaadt je imago, dat van je team en uiteindelijk het imago van de SVB. Het is mogelijk zelfs strafbaar.

De Gedragscode is geen statisch document: het zal voortdurend worden aangepast aan voortschrijdende inzichten en ontwikkelingen (bijvoorbeeld op het gebied van ICT en Informatiebeveiliging en veranderende wet- en regelgeving). Deze Gedragscode bevat handvatten waarmee je kunt bepalen wat toelaatbaar is en wat niet en wat van jou verwacht wordt als professional.
Zo wordt op pagina 15 aandacht besteed aan de afspraken met betrekking tot flexibel werken. De laatste paragraaf op pagina 29 brengt nog enkele huisregels onder je aandacht.
De SVB staat garant voor een professionele en onvoorwaardelijk transparante houding ten opzichte van opdrachtgevers, klanten en medewerkers en verwacht dit ook van jou.

Voor wie is deze code bestemd?

De Gedragscode geldt voor iedereen die bij de SVB werkt, of die werkzaamheden verricht voor de SVB. Deze code geldt dus ook voor een uitzendkracht, stagiair, gedetacheerde, externe adviseur, medewerkers van de cateraar, etc.

De Gedragscode als leidraad

De Gedragscode kan nooit in elke denkbare situatie voorzien, maar doet een beroep op verantwoord, vertrouwelijk, transparant, zorgvuldig en onpartijdig handelen van medewerkers[1].

Integriteit gaat pas werkelijk leven in de dagelijkse praktijk en in de gesprekken die je met elkaar hierover voert. Waar loop je in jouw functie tegenaan en welk handelen wordt er in die situatie van je verwacht? Het is heel normaal dat je daarbij soms twijfelt. Normen en waarden zijn niet altijd duidelijk toepasbaar en kunnen ook strijdig zijn met elkaar. Bovendien wijzigen de omstandigheden voortdurend door nieuwe ontwikkelingen. Je moet dus altijd zelf blijven nadenken. Je bent en blijft zelf verantwoordelijk voor je handelen, maar je hebt wel een kader nodig waaraan je jouw handelen kunt toetsen.

Het is goed om met elkaar, bijvoorbeeld in een werkoverleg, dilemma's en de Gedragscode te bespreken. In de E-learning module wordt hier ook aandacht aan besteed. Verder zal de Gedragscode regelmatig worden aangepast aan ontwikkelingen binnen en buiten de SVB.

[1] Daar waar in de gedragscode wordt gesproken over 'medewerker', bedoelen we de hele doelgroep voor wie de code geldt.

Integriteit als speerpunt en voorbeeldfunctie leidinggevenden

Integriteit moet bij ons allemaal 'tussen de oren zitten' en hoort thuis in alle aspecten van het werk. De leidinggevenden hebben hierin het voortouw en hebben tot taak om het integriteitsbeleid actief uit te dragen in woord en daad. Alleen door zelf het goede voorbeeld te geven kun je geloofwaardig zijn.
Als leidinggevende is het van belang integriteitsrisico's tijdig te herkennen, bespreekbaar te maken en op de juiste manier aan te pakken. Medewerkers die niet integer gedrag aan de orde stellen horen te worden gesteund en waar nodig beschermd. Alleen dan kunnen medewerkers zich veilig genoeg voelen om elkaar en de leiding aan te spreken op niet integer gedrag.

Bovenstaande betekent dat de SVB als werkgever ook een verantwoordelijkheid heeft. Zij dient leidinggevenden in staat te stellen en waar nodig te begeleiden om hun rol naar behoren te kunnen vervullen.

Bespreken, signaleren en melden

Voortdurende aandacht voor integriteit is nodig. SVB hecht veel waarde aan het bespreekbaar maken. Het is van belang dat leidinggevenden met elkaar dilemma's bespreken. Collegiaal beraad tussen leidinggevenden onderling is belangrijk om te toetsen of er op een juiste manier invulling wordt gegeven aan de rol van de leidinggevenden.
Maar ook is het goed om in de teams zelf dilemma's te delen.
Bij transparantie en zorgvuldigheid hoort ook elkaar aanspreken. Dit moet wel op een veilige manier kunnen gebeuren.

Het uitgangspunt van elkaar aanspreken en hoe je niet integer handelen en ongewenste omgangsvormen kunt of moet melden, lees je op pagina 26 van deze Gedragscode.

Handhaving en sancties

Het is belangrijk dat iedereen zich aan de code houdt. Bij overtreding worden disciplinaire maatregelen getroffen conform de CAO SVB. Deze disciplinaire maatregelen variëren van een waarschuwing tot ontslag. Bij misdrijven zal ook aangifte worden gedaan bij het Openbaar Ministerie.
Voordat tot het opleggen van een sanctie wordt overgegaan, zal eerst gedegen onderzoek moeten plaatsvinden. De feiten moeten op deugdelijke wijze worden vastgesteld en er moet rekening worden gehouden met relevante omstandigheden. Daarbij moet sprake zijn van hoor en wederhoor, zorgvuldige verslaglegging en – voor zover van toepassing een evenredige inzet van onderzoeksmiddelen.

Specifieke normen en regels rondom integer handelen

Onder *niet* integer handelen vallen meerdere categorieën. Strafbare feiten als corruptie, fraude, diefstal en vandalisme zijn duidelijk in strijd met integer gedrag. Ook belangenverstrengeling, misbruik van bevoegdheden of positie is in strijd met integer handelen. Andere vormen zoals gedrag of handelingen die vallen onder ongewenste omgangsvormen, of handelingen die strijdig zijn met regels rond informatiebeveiliging en fysieke beveiliging zullen ieder in een aparte paragraaf worden toegelicht.

Omgaan met relaties en relatiegeschenken

Geschenken, giften en gunsten die je in je functie ontvangt, meld je aan je leidinggevende zodat ze geregistreerd kunnen worden. Een geschenk met een waarde van maximaal € 50,-, hoeft niet te worden geregistreerd en

mag gehouden worden. Je meldt wel bij je leidinggevende dat je het ontvangen hebt. Iedere directie registreert de overige geschenken zelf. De registratie heeft tot doel na te kunnen gaan waar of bij wie de relatiegeschenken terecht zijn gekomen. De directie HR, Inkoop & Facilities heeft een format dat voor deze registratie gebruikt wordt. De leidinggevende besluit hoe moet worden omgegaan met het geschenk, de gift of de gunst. Ze zijn eigendom van de SVB. Over aangeboden geschenken en dergelijke maak je altijd afspraken met je leidinggevende.

In aanvulling daarop geldt:

- Je mag nooit geschenken aannemen van relaties met wie de SVB op dat moment in onderhandeling verkeert. Ook mag je nooit geschenken op jouw huisadres aannemen.
- Als de waarde van het geschenk, de gift of de gunst niet in verhouding staat tot het werk wat er voor gedaan is, mag het niet worden aangenomen. Ook bij twijfel over de waarde overleg je met je leidinggevende.
- Als er aan het geschenk, de gift of de gunst een voorwaarde is gekoppeld, mag het niet worden aangenomen.
- Wanneer je namens de SVB een geschenk aan derden (waaronder klanten) wenst aan te bieden, moet je vooraf toestemming hebben van je leidinggevende, waarbij je het SVB belang vooraf moet kunnen verantwoorden. De leidinggevende besluit hoe hiermee om te gaan. De criteria die gelden bij aanname van een geschenk, gift of gunst gelden hier op gelijke wijze.

Uitnodigingen

Je mag een uitnodiging voor een lunch, diner, concert of (sport) evenement van een relatie van de SVB uitsluitend accepteren als je kunt aantonen dat daarmee het belang van de SVB wordt gediend. Zulke uitnodigingen bespreek je met je leidinggevende. De leidinggevende

neemt hierover een besluit. Als je een relatie van de SVB uitnodigt voor een lunch of diner, waarvan de kosten bij de SVB worden gedeclareerd, moet je het belang kunnen verantwoorden dat de SVB heeft bij deze uitnodiging. De leidinggevende neemt hierover een besluit. De criteria die gelden bij aanname van een geschenk, gift of gunst gelden hier op gelijke wijze.

Geen misbruik maken van positie, faciliteiten of informatie

Je mag je niet laten leiden door eigen belang of oneigenlijke motieven. Je bent betrouwbaar en zorgvuldig en aanspreekbaar op jouw gedrag. Je maakt geen misbruik van je positie, van faciliteiten die je tot je beschikking hebt, of van informatie waarover je beschikt om een (toekomstig) persoonlijk voordeel te behalen voor jezelf, maar ook niet voor bijvoorbeeld je partner, vrienden of een collega. Je behartigt geen belangen van klanten waarmee je een privérelatie hebt, je behandelt geen dossiers waar je een persoonlijk belang in hebt of kunt hebben. Je benadeelt klanten niet. Je vermijdt (ook de schijn van) belangenverstrengeling.

Inkoop, aanbesteding en inhuur van externen (draaideurconstructies)

Als je binnen je functie betrokken bent bij inkoop-, aanbestedings- en/of inhuurprocedures en persoonlijke betrekkingen hebt met een aanbieder van diensten, meld je dit onmiddellijk bij je leidinggevende. De leidinggevende neemt hierover een besluit. Voorkom ongewenste belangenverstrengeling te allen tijde bij inhuur. Zo kunnen er nooit externen worden ingehuurd van een bedrijf waarin een SVB-medewerker een persoonlijk belang heeft. Verder neem je van een aanbieder geen faciliteiten of diensten aan die jouw onafhankelijke positie ten opzichte van de aanbieder kunnen beïnvloeden.

(Betaalde) nevenwerkzaamheden

Je vraagt bij je leidinggevende vooraf schriftelijke toestemming om tegen beloning arbeid voor derden te verrichten dan wel als zelfstandige werkzaamheden te verrichten. Zonder schriftelijke toestemming mag je geen betaalde nevenwerkzaamheden verrichten. Bijvoorbeeld op grond van bepalingen uit de arbeidstijdenwet kunnen er voorwaarden worden verbonden aan de toestemming.
Soms zijn onbetaalde nevenwerkzaamheden van dien aard dat het goed is om dat met je leidinggevende te bespreken of dat samen kan gaan met je werk voor de SVB. Dat is bijvoorbeeld het geval als ze op enigerlei wijze kunnen leiden tot belangenverstrengeling, of kunnen conflicteren met je werkzaamheden voor de SVB. Kijk dan met je leidinggevende en HR-adviseur naar een passende oplossing.

Voorbeelden: Het (eenmalig) op persoonlijke titel schrijven van een artikel dat verwant is aan je SVB functie. Of als ZZP-er of vrijwilliger PGB-klanten adviseren of hun belangen behartigen, terwijl je ook als dossierbehandelaar bij de SVB deze dossiers kunt inzien.

Privé(relaties)

Soms gaan werk en privé door elkaar lopen, bijvoorbeeld doordat je een relatie krijgt met een collega. Dat hoeft geen probleem te zijn, als je er transparant over bent naar je leidinggevende en ervoor zorgt dat deze relatie het uitvoeren van je functie of de aan jou opgedragen taken niet belemmert en niet leidt tot ongepast gedrag.

Het is belangrijk je leidinggevende op de hoogte te stellen.
De leidinggevende bespreekt met HR Advies of er door deze privérelatie veranderingen in je (onafhankelijke) positie optreden. Voorbeelden hiervan zijn als je als staffunctionaris een relatie hebt met een manager, waarbij je datzelfde management ook regelmatig adviseert, of als je als manager een

relatie hebt met een medewerker uit dezelfde directie of als een van beiden een controlerende functie ten opzichte van de ander heeft. In ieder geval kunnen bij een hiërarchische arbeidsverhouding de partners niet in dezelfde functieverhouding blijven werken.

De (naast hogere) leidinggevende bepaalt welke invloed de relatie op het functioneren van beiden op het werk kan hebben. Als de relatie van invloed is op jouw onafhankelijke positie of op die van de ander waarmee een relatie is aangegaan dan zoekt de leidinggevende in samenwerking met HR Advies naar een andere positie voor jou of de ander. Als je hier niet aan meewerkt, kan dit tot ontslag leiden.

Privégebruik van SVB-voorzieningen

Gebruik van eigendommen of voorzieningen van de SVB voor privédoeleinden is in principe niet toegestaan. Bepaalde *algemene* voorzieningen mogen, als dat gebruik incidenteel, kortstondig en gepast is, wel worden benut, mits dit niet storend is voor de dagelijkse werkzaamheden. Het gebruik mag ook de continuïteit van het primair proces en/of de bedrijfsvoering niet in gevaar brengen. Misbruik, d.w.z. overmatig, uitbundig, onnodig, storend of schadelijk privégebruik is nooit toegestaan.

Voorbeelden:

- *Een telefoontje plegen naar de school van je kind is prima. Met een SVB-telefoon/abonnement betaalde commerciële telefoonnummers bellen om te stemmen voor een tv-programma of uitvoerig bellen met een bekende die in het buitenland verblijft is niet toegestaan.*
- *Een online SVB-voorziening als routenet voor een privé-rit raadplegen is prima. Een applicatie met bedrijfsspecifieke en/of vertrouwelijke informatie (o.a. klantsystemen van PGB (zoals TREKS) of SUWI-net) voor eigen gebruik raadplegen is nooit toegestaan en is ten strengste verboden en kan leiden tot ontslag op staande voet.*

- *Dat je een SVB pen ook gebruikt om wat andere aantekeningen te maken is natuurlijk prima, een beamer lenen voor een vergadering op je sportvereniging gaat te ver, dat doe je natuurlijk niet.*

Bij twijfel, bespreek het dan eerst met je leidinggevende.

Waardevolle spullen zoals mobiele telefoons, laptops, tokens en andere informatiedragers

Een mobiele telefoon, tablet, laptop of token die de SVB heeft verstrekt, is bestemd voor zakelijk gebruik. Deze apparaten blijven eigendom van de SVB. Waardevolle spullen behandel je met zorg. Je laat ze niet onbeschermd achter, ook niet thuis of in een auto. Heb je deze zaken niet langer nodig voor de uitvoering van je werkzaamheden, dan lever je ze in bij de SVB. Dit doe je uit eigen beweging, maar zeker ook als de SVB erom verzoekt dien je ze onmiddellijk in te leveren. Deze zaken zijn immers altijd eigendom van de SVB gebleven.
Controle op het onrechtmatig meenemen van eigendommen kan steekproefsgewijs plaatsvinden of bij vermoeden/verdenking van diefstal. Zo nodig kan de inhoud van dozen, tassen en dergelijke gecontroleerd worden.

Bring Your Own Device (BYOD)

Als je met privé -apparatuur werk verricht voor de SVB of op systemen van de SVB inlogt, zorg je dat je dit veilig doet. Je beveiligt de apparatuur tegen: gebruik door onbevoegden, spam, virussen, etc. Je plaatst een wachtwoord op alle apparatuur waarop je informatie, gegevens van de SVB hebt opgeslagen of waarmee je deze binnenkrijgt of waarmee je deze kunt benaderen. Je gebruikt alleen legale software om werk voor de SVB te verrichten. Je volgt aanwijzingen van de SVB op.

De SVB kan niet aansprakelijk worden gesteld voor vermissing van en/of schade aan privé-eigendommen.

Vergoedingen en dergelijke

Je declareert geen kosten die niet gemaakt zijn, of al op een andere wijze zijn of kunnen worden vergoed. Als je bijvoorbeeld al een vergoeding van je zorgverzekeraar hebt ontvangen voor een beeldschermbril en je declareert vervolgens eveneens de volledige kosten aan de SVB, dan pleeg je fraude en zullen er disciplinaire maatregelen worden genomen.

Wat verstaan we onder ongewenste omgangsvormen?

Ongewenste omgangsvormen tasten de waardigheid en/of lichamelijke integriteit van een medewerker aan. Dit gedrag wordt niet getolereerd binnen de SVB. Het past niet bij hoe we binnen de SVB met elkaar willen omgaan. Bovendien schaadt het, het welzijn en/of de gezondheid van medewerkers. Ze worden door de medewerker, die het doelwit is van dit gedrag, als ongewenst ervaren. Behandel de ander zoals je zelf behandeld wilt worden.

Bij ongewenste omgangsvormen kan het gaan om handelingen van een groep of een individu, gericht tegen een persoon of personen die dit als bedreigend, vernederend of intimiderend ervaart/ervaren. Iedere medewerker maakt voor zichzelf uit of hij een opmerking of handeling als vervelend en dus ongewenst ervaart. Zowel de beleving van de individuele medewerker, als algemene normen en waarden van gepast gedrag zijn daarbij doorslaggevend. Ongewenst gedrag en ongewenste omgangsvormen in de zin van seksuele intimidatie, agressie, geweld en/of discriminatie zijn niet toegestaan en zijn in welke vorm dan ook (ook via social media, e-mail etc.) onacceptabel.

Het is niet mogelijk een uitputtende opsomming te geven van ongewenste gedragingen. Om toch enig inzicht te geven, zijn de volgende categorieën

benoemd: verbale agressie (bijvoorbeeld schelden, schreeuwen, treiteren); fysieke agressie (bijvoorbeeld slaan, vastgrijpen); psychische agressie/ intimidatie (bijvoorbeeld dreigen, chanteren, achtervolgen, pesten/ 'mobbing' en/of stalken); seksuele intimidatie (bijvoorbeeld nafluiten, opmerkingen maken, aanranding).

Discriminatie

Discriminatie is het ongelijk behandelen en achterstellen van mensen op basis van kenmerken die er niet toe doen in een situatie.

Discriminatie is niet het maken van onderscheid op zich, maar het maken van verboden onderscheid. Dat wil zeggen: onderscheid maken tussen mensen, zonder dat daarvoor objectief een goede reden is.

Het is verboden onderscheid te maken op grond van:

- Ras
- Levensovertuiging
- Nationaliteit
- Leeftijd
- Handicap of chronische ziekte
- Arbeidsrelatie (full-/parttime)
- Sekse
- Godsdienst
- Seksuele geaardheid
- Politieke gezindheid
- Arbeidscontract (onbepaald/tijdelijk)
- Burgerlijke staat

Discriminatie uit zich in bijvoorbeeld pesten, uitsluiten, intimideren, maar ook zaken als ongelijke beloning.
Op intranet onder MijnHR/ SVB Gedragscode en (on)gewenst gedrag/ Discriminatie vind je de discriminatiegronden verder uitgewerkt met voorbeelden.

Gevolgen

Medewerkers die zich gediscrimineerd voelen of slachtoffer zijn van ongewenste omgangsvormen ervaren vaak stress. Stress kan leiden tot

psychische en fysieke klachten en uiteindelijk tot uitval. Ook is de kans groot dat medewerkers gedemotiveerd raken, minder presteren. Dat maakt, na bijvoorbeeld langdurige uitval, de stap terug naar werk extra moeilijk.

Heb je te maken met een dergelijke situatie, lees dan verder op pagina 26 om te zien wat je hieraan kunt doen.

Vertrouwenspersonen en Bedrijfsmaatschappelijk werkers (BMW)

Bij incidenten die als ongewenste omgangsvormen zijn aan te duiden, spelen vertrouwenspersonen en de BMW naast de HR-adviseur een belangrijke rol. Zij adviseren en begeleiden medewerkers bij integriteitsincidenten. Vooral bij ongewenste omgangsvormen zijn zij een adequate eerste opvang. Vanwege het zeer persoonlijke karakter kan de vertrouwenspersoon, de BMW of de HR-adviseur ook extra ondersteuning bieden. Meer informatie vind je op intranet.

Als je te maken krijgt met een schending zoals omschreven in deze Gedragscode kun je naast de HR-adviseur ook terecht bij een vertrouwenspersoon of BMW. Op intranet vind je een overzicht van de vertrouwenspersonen en de BMW's. Vertrouwenspersonen en BMW kunnen advies geven over hoe om te gaan met een incident en/ of serieuze aanwijzing van een integriteitsschending. Daarnaast kunnen vertrouwenspersonen of BMW doorverwijzen naar externe deskundigen of naar de HR-adviseur. Zij kunnen begeleiden in het oplossingstraject en ze verlenen nazorg. Wat je met vertrouwenspersonen of BMW bespreekt blijft vertrouwelijk (tenzij je daar samen met de vertrouwenspersoon of BMW andere afspraken over maakt of als de wet anders voorschrijft).

Hoe ga ik om met informatie?

Medewerkers dienen zorgvuldig met informatie om te gaan. Het belang van zorgvuldige informatieoverdracht en informatiebeveiliging is door de toenemende digitalisering en de komst van nieuwe media (zoals, internet en social media) steeds groter geworden. Dit betekent dat je de spelregels die gelden rondom informatiebeveiliging altijd in acht dient te nemen. Deze regels zijn te vinden op het intranet van de SVB (portal Informatiebeveiliging).

Wees je bewust van je eigen gedrag en handelen. Zorg dat niemand ongewenst kan meekijken op (digitale) werkdocumenten of kan meeluisteren met zakelijke gesprekken.
Let op wat je wel of niet kan bespreken (ook aan de telefoon) in bijvoorbeeld de trein of op andere (openbare) plaatsen buiten de SVB, maar ook thuis. Dit geldt ook voor het gebruik van een laptop of andere devices in openbare, of op andere plaatsen (ook bij ketenpartners) waar anderen mogelijk ongewenst kunnen meekijken of -luisteren. Werk onderweg ook niet met klant- en of persoonsgegevens. Zakelijke documenten gooi je weg op kantoor in de daarvoor bestemde afgesloten bakken.
Andere informatiedragers moeten via IT worden afgevoerd.
Bovendien dien je zorgvuldig om te gaan met social media als het werk gerelateerde informatie betreft. Deze voorbeelden zijn niet uitputtend.

Flexibel werken

In 2018 zullen alle SVB medewerkers worden voorzien van een mobiele SVB-device waarmee flexibel en veilig op kantoor maar ook daarbuiten kan worden gewerkt. Mag je flexibel werken? Dan dien je eerst zorgvuldig kennis te nemen van de “Regeling flexibel werken” vòòrdat je hiermee start en maak je hierover goede afspraken met je leidinggevende.
De benodigde informatie is te vinden op het intranet van de SVB (Handboek HR: Regeling flexibel werken en de portal Informatiebeveiliging).

Spelregels voor informatiebeveiliging

SVB-ers zijn terughoudend met het delen van informatie. Informatie die je in het kader van de uitvoering van je werkzaamheden vergaart en gebruikt moeten strikt zakelijk worden behandeld.
Je gaat bij het uitvoeren van je werk zorgvuldig om met gevoelig informatiemateriaal en de privacy van zowel klanten als van collega's.
Je handelt volgens de Algemene Verordening Gegevensbescherming (AVG) (voorheen de Wet bescherming persoonsgegevens).

We maken onderscheid in vertrouwelijke informatie en geheime informatie:

- informatie moet als vertrouwelijk worden aangemerkt wanneer onbedoeld openbaar worden, negatieve gevolgen kan hebben en/of als de informatie betrekking heeft op een persoon (persoonsgegevens). Deze informatie is bedoeld voor een beperkte groep en wordt alleen verspreid naar een specifieke doelgroep. Voorbeelden van vertrouwelijke informatie zijn: passwords, persoonsgegevens, klantgegevens, contracten en begrotingsonderhandelingen.
- informatie moet onder bepaalde bijzondere omstandigheden worden aangemerkt als 'geheim'. Dit is nodig wanneer geheime informatie onbedoeld openbaar wordt en mogelijk **zeer ernstige** negatieve gevolgen kan hebben voor de SVB. Kenmerkend is dat deze informatie bedoeld is voor een zeer specifieke en kleine doelgroep. Verspreiding van deze informatie wordt beheerd en is gedocumenteerd. Een voorbeelden van geheime informatie is onderzoeksinformatie.

Voor zowel vertrouwelijke als geheime informatie geldt dat er sprake is van een geheimhoudingsplicht. Vertrouwelijke en geheime informatie mag alleen worden verstrekt aan de rechtmatige bron, of aan collega's die deze informatie nodig hebben voor de uitoefening van hun taken of om te voldoen aan een wettelijke verplichting. Bij openbaarmaking of het

ongeoorloofd delen van deze informatie ontstaat schade voor de SVB en mogelijk ook voor anderen. Hoe weet je welke informatie vertrouwelijke of geheime informatie is? Een goede praktijk is om aan te nemen dat alle persoonsgegevens en alle informatie die je over de SVB en haar activiteiten heeft vertrouwelijk of geheim is, tenzij het tegendeel duidelijk is.

Je bepaalt of iemand de informatie werkelijk nodig heeft en ook rechtmatig mag gebruiken voor de uitvoering van zijn werk. Indien dat niet het geval is, geef je de informatie niet. Bij twijfel verwijs je de vrager door naar je leidinggevende. Je voorkomt dat anderen toegang kunnen krijgen tot de informatie. Je slaat de informatie alleen op in een map met beperkte toegangsrechten en je zorgt dat de vertrouwelijke en geheime informatie niet kan worden gewijzigd. Je laat de vertrouwelijke en geheime informatie niet onbeheerd achter, los op je bureau of in een niet afgesloten kast. Stuur eveneens geen vertrouwelijke of geheime informatie, inclusief interne communicatie, zoals intranetpostings, buiten de SVB (inclusief je eigen persoonlijke e-mailadres), tenzij dit toegestaan wordt volgens de geldende wet- en regelgeving.

Je gaat bij het uitvoeren van je werk zorgvuldig om met gevoelig informatiemateriaal en de privacy van zowel klanten als van collega's.

Je mag als werknemer geen inbreuk maken op de intellectuele eigendomsrechten van de SVB. Uiteraard doe je dat ook niet na beëindiging van je dienstverband bij de SVB.

Verwerken van persoonsgegevens

Bij het verwerken van financiële en persoonlijke informatie over burgers, collega's of anderen met wie SVB te maken heeft, dien je als medewerker de volgende principes in acht te nemen:

- verzamel, gebruik en bewaar alleen de persoonlijke gegevens die nodig zijn voor de uitvoering van de dienstverlening.

- beperk de interne toegang tot persoonlijke informatie aan personen tot situaties dat er een legitieme zakelijke reden is om deze informatie in te zien. Gebruik alleen persoonlijke informatie voor de doeleinden waarvoor het oorspronkelijk is verkregen. Verkrijg de toestemming van de betrokkene alvorens persoonlijke gegevens extern te delen, tenzij de verstrekking wettelijk is voorgeschreven.
- persoonsgegevens worden nooit gedeeld via social media, ook niet via een persoonlijk bericht en ook niet als de klant zelf al persoonlijke gegevens via dat kanaal heeft gedeeld. Informatie wordt gedeeld via de toegestane kanalen die wel voldoende veilig zijn.

Datalekken

Medewerkers hebben de plicht om eventuele geconstateerde datalekken intern te melden (conform de hiervoor opgestelde procedures). Een datalek is een "inbreuk in verband met persoonsgegevens": een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

Naast de mogelijkheid tot het melden van datalekken heeft SVB (in de vorm van de Functionaris Gegevensbescherming (FG)) eveneens een vertrouwelijk aanspreekpunt met betrekking tot het verwerken van persoonsgegevens. De FG kan door alle medewerkers worden benaderd voor eventuele zaken met betrekking tot het verwerken van persoonsgegevens.

Gegevens Functionaris Gegevensbescherming (FG)
06-15831736
FG@svb.nl

ICT voorzieningen

De ICT voorzieningen, zoals informatiesystemen, software, verbindingen en applicaties zijn voor zakelijk gebruik ter beschikking gesteld en mogen alleen door jou gebruikt worden. De omschrijving van ICT-voorzieningen is niet limitatief en kan worden aangevuld met faciliteiten zoals deze in de toekomst door de SVB ter beschikking worden gesteld. Het is toegestaan om incidenteel en kortstondig de algemene beschikbare voorzieningen (zoals telefoon of internet) voor persoonlijke doeleinden te gebruiken, mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk. Dat kan dus nooit betrekking hebben op bedrijfsinformatiesystemen etc. Deze specifieke voorzieningen mogen altijd alleen maar worden gebruikt voor zover opgedragen en noodzakelijk voor de uitoefening van je werkzaamheden.

Voorbeeld: Je kijkt op buienradar voordat je op de fiets naar huis stapt, dat is prima. Maar los van dossierbehandeling inkomensgegevens van bekenden opzoeken in een van onze informatiesystemen mag nooit.
Zoals eerder aangegeven, het raadplegen van (informatie)systemen waarin klantgegevens zijn opgenomen, gebeurt alleen voor zover dat noodzakelijk is voor de uitvoering van je werkzaamheden. Niet-werkgerelateerd raadplegen is uit den boze en wordt gesanctioneerd. Een dergelijke overtreding kan leiden tot ontslag op staande voet.

Gebruik van ICT-voorzieningen dient binnen de grenzen van de wet plaats te vinden (in het bijzonder zijn diefstal, fraude, ongeautoriseerd binnendringen in computersystemen van derden, schending van het auteursrecht, het (intellectueel) eigendomsrecht en valsheid in geschrifte verboden). De continuïteit van het primair proces en/of de bedrijfsvoering van de SVB mag nimmer in gevaar komen. Je gaat op een zorgvuldige en vertrouwelijke wijze om met (eigen) wachtwoord(en), zoals met je eigen pincode. Dit houdt in dat de toegekende of zelf bepaalde wachtwoorden

geheim zijn en niet aan collega's en/of aan derden bekend mogen worden gemaakt. De toegekende gebruikersnaam is persoonlijk. Je bent zelf verantwoordelijk voor wat er met de eigen gebruikersnaam wordt gedaan en dit mag dus niet worden overgedragen aan anderen.

Als je een (software-)token of app hebt gekregen voor toegang tot een netwerk (Remote Access), of een applicatie, ga je daar net zo mee om als met je eigen gebruikersnaam en wachtwoord. Je ontvangt daarbij aanvullende instructies die je ook opvolgt.

Ook voor het gebruik van speciale apparatuur (zoals laptop en tablet) houd je je aan de daarvoor geldende aanvullende instructies.

Het is niet toegestaan om de beschikbare ICT voorzieningen te gebruiken in strijd met belangen van de SVB. Dit betekent dat het onder meer niet is toegestaan om:

- dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende berichten/ bestanden intern (binnen de SVB) te bewaren, te versturen of uit te printen;
- externe (illegale, gratis voor individueel gebruik, etc.) software en applicaties te downloaden, in te lezen en te installeren op de computer of het netwerk, tenzij dit uitdrukkelijk is toegestaan door de leidinggevende en noodzakelijk is voor het uitoefenen van de functie;
- bewust virussen te verspreiden via het netwerk;
- laptops en personal computers die niet door de SVB zijn geconfigureerd op het netwerk (proberen) aan te sluiten, tenzij dit uitdrukkelijk is toegestaan door de directie en noodzakelijk is voor het uitoefenen van de functie.

Deze lijst met voorbeelden is niet uitputtend. Werknemers die belast zijn met informatiebeveiliging en andere specifieke taken hebben, kunnen vanuit hun functie soms andere bevoegdheden hebben, hiervoor is dan expliciet toestemming gegeven.

E-mail en internet zijn voor zakelijk gebruik ter beschikking gesteld. Hiervoor gelden dezelfde richtlijnen als voor zakelijk gebruik van ICT voorzieningen. Het is niet toegestaan om e-mail/ internet te gebruiken in strijd met de belangen van de SVB. Dit betekent dat het onder meer niet is toegestaan om:

- dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende berichten intern (binnen de SVB) of extern (buiten de SVB) te bekijken, te verzenden, door te sturen of te bewaren;
- deel te nemen aan kettingberichten of niet zakelijke nieuwsgroepen, nieuwsbrieven of abonnementen;
- berichten anoniem te versturen of onder een fictieve dan wel valse naam;
- bijlagen van verdachte e-mailtjes te openen;
- links in e-mails aan te klikken, waarin gevraagd wordt vertrouwelijke of geheime informatie/ gegevens (zoals wachtwoorden bij de SVB, klantgegevens) in te vullen (Phishing);
- internetsites die seksueel getint, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten te bezoeken of dergelijk materiaal te bekijken of te downloaden;
- internetsites die kunnen leiden tot herhaald gebruik zoals sites die beursberichten bevatten, te bezoeken, te bekijken of materiaal daarvan te downloaden, tenzij dit uitdrukkelijk is toegestaan door de leidinggevende en noodzakelijk is voor het uitoefenen van de functie;
- films of muziek te downloaden tenzij deze nodig zijn voor of bij de uitoefening van je functie en dit is toegestaan door je leidinggevende.
- vertrouwelijke of geheime informatie mag per e-mail worden verzonden mits je dit zorgvuldig en op een door de SVB voorgeschreven wijze doet.

  Voorzie de e-mail van de categorisering vertrouwelijk of persoonlijk. Het wordt aanbevolen in plaats van de documenten een link naar het document te sturen of het document te voorzien van een wachtwoord en dit wachtwoord persoonlijk (niet via e-mail) aan de ontvanger door te geven.

Deze lijst met voorbeelden is niet uitputtend. Verboden e-mail- en internetgebruik wordt door de SVB zoveel mogelijk technisch onmogelijk gemaakt.

Communicatie op internet en sociale media

Een opmerking of mening op internet is snel geplaatst. Je hebt vervolgens geen controle over wat er mee gebeurt, ook niet binnen afgeschermde internetomgevingen. Jouw gepubliceerde 'reply', 'tweet' of 'comment' kan in korte tijd worden doorgestuurd naar andere mensen of worden doorgeplaatst naar andere sites. Op internet blijft altijd alles opvraagbaar en door koppelingen tussen verschillende (sociale) netwerken is jouw relatie met de SVB makkelijk gelegd.
Het onderscheid tussen zakelijk en privé is dus dun op internet. Je bent al snel – soms onbewust – het 'gezicht' van de organisatie. Om mogelijke schade aan jezelf en anderen te voorkomen staan hierna een aantal tips. Zij kunnen je helpen je meer bewust te zijn van de mogelijkheden en risico's bij online communicatie.

- Geef geen interne of persoonlijke informatie vrij over de SVB, klanten, collega's of anderen waarmee je in contact bent.
- Wees je bewust dat je (persoonlijke) mening gevolgen kan hebben voor de SVB. Jij bent verantwoordelijk voor dat wat je schrijft of publiceert op internet.
- Valt een discussie buiten je expertise of twijfel je over je antwoord? Reageer dan niet meteen, maar overleg eerst over de juiste aanpak met de Directie Communicatie en Voorlichting .
- Reageer niet op negatieve berichten over de SVB. Stel de Directie Communicatie en Voorlichting (communicatie@svb.nl) op de hoogte en laat een eventuele reactie over aan de woordvoerder van de SVB.
- Vraagt iemand om een quote, mening of interview over een SVB-gerelateerd onderwerp? Neem dan, net als gebruikelijk bij de gedrukte

media, contact op met de perswoordvoerder van de SVB (communicatie@svb.nl)
- Ook als je het niet eens bent met een ander, blijf professioneel en respectvol.
- Zorg dat het duidelijk is wie je bent en vanuit welke rol je reageert.

Wat verwachten we van je op het gebied van fysieke beveiliging?

Fysieke beveiliging gaat over arbeidsveiligheid in de ruimste zin van het woord. Alertheid van medewerkers speelt daarbij een belangrijke rol. Aandachtspunten zijn onder meer: brand, ongevallen, arbeidsomstandigheden (veiligheid), noodplannen, bedrijfscontinuïteit en bedrijfshulpverlening (BHV). Het is belangrijk dat iedereen zijn werk binnen de SVB kan doen zonder dat hij bang hoeft te zijn voor zaken als diefstal, vernieling, of andere onaanvaardbare of zelfs criminele activiteiten. Om de veiligheid te waarborgen volg je bij (kleine) ongevallen en calamiteiten de instructies van de BHV op. Daarnaast zorg je dat je bekend bent met de beveiligingsregels en (preventieve) beveiligingsmaatregelen van de SVB locatie waar je werkt.

Toegang tot de SVB

De toegang tot het gebouw wordt geregeld met behulp van een toegangsbeheersysteem.
Het is niet toegestaan een toegekende toegangspas aan anderen te verstrekken. De toegekende toegangspas is persoonlijk en wordt ook alleen persoonlijk gebruikt. Het is daarnaast nimmer toegestaan anderen te laten meelopen met een toegangspas.

Hoe houden wij de vinger aan de pols?

De SVB werkt op basis van vertrouwen. Normaal gesproken kijkt niemand over je schouder mee bij e-mail- en internetgebruik. Het is wel zo dat door voortschrijdende technologische ontwikkelingen en de steeds zwaardere eisen die aan informatiebeveiliging worden gesteld, de SVB permanente maatregelen heeft moeten treffen om klantgegevens veilig te verwerken en te bewaren, alsmede zichzelf te beschermen tegen kwaadwillenden die digitaal willen inbreken of de continuïteit van de SVB willen verstoren. Om die reden worden afwijkingen in systemen gedetecteerd en onderzocht door het SVB Security Operations Center (SOC). In dat kader wordt ook gebruik gemaakt van gelogde gegevens die nader kunnen worden onderzocht door het SOC.

Controle gebruik voorzieningen

Het gebruik van ICT voorzieningen, waaronder internet en e-mail, wordt op geautomatiseerde en geanonimiseerde wijze gecontroleerd.
De redenen hiervoor zijn: vooral systeem- en netwerkbeveiliging (door het SOC); verzamelen van bewijs van zakelijke transacties of dossiervorming ten behoeve van de bedrijfsvoering; maar ook het voorkomen van negatieve publiciteit; tegengaan van ongewenst gedrag (zoals seksuele intimidatie); controle op naleving van de gedragsregels; kosten- en capaciteitsbeheersing.

Vanuit hun verantwoordelijkheid voor systeem- en netwerkbeveiliging monitort en onderzoekt het SOC afwijkingen in systemen ter voorkoming van, om in te grijpen bij, en inzage te geven in (ernstige) IT-beveiligingsincidenten, kwetsbaarheden en dreigingen. Het SOC handelt daarbij overeenkomstig het SOC-mandaat.

Onderzoeken gericht op personen, vinden alleen plaats wanneer er een nadrukkelijk vermoeden bestaat van een schending van de regels of de

Gedragscode, waarbij het belang van de werkgever om te onderzoeken wordt afgewogen tegen het belang van het individu. Zo nodig kan vervolgens een gericht onderzoek naar een persoon worden uitgevoerd. De omvang van een dergelijk onderzoek wordt daarbij steeds zo beperkt mogelijk gehouden.
Dit betekent onder meer dat de controle zo gericht mogelijk zal plaatsvinden, dat de duur van de controle zoveel mogelijk wordt beperkt en dat slechts in uitzonderlijke gevallen zal worden overgegaan tot kennisneming van de inhoud van e-mail- of internetgebruik.

Een verzoek tot een dergelijke controle of onderzoek wordt door de directeur schriftelijk en gemotiveerd gedaan aan de Raad van Bestuur. Na beoordeling van een dergelijk verzoek, kan de Raad van Bestuur, de directeur van het IT Bedrijf opdracht geven de gevraagde gegevens te leveren. Persoonsgegevens over gebruik van ICT voorzieningen worden niet langer bewaard dan noodzakelijk, met een maximum bewaartermijn van 13 maanden, tenzij een langere bewaartermijn nodig is in het kader van een gericht onderzoek en/of te treffen maatregelen.
De medewerker tegen wie het onderzoek is gericht, wordt daarvan (op een nader te bepalen tijdstip) op de hoogte gesteld.

Om de medewerkers en de SVB te kunnen beschermen wordt er op alle locaties gebruik gemaakt van videocamera's. Bijvoorbeeld ter ondersteuning van de intercom bij toegangsverlening, voor de beveiliging van medewerkers in de 'winkel' of op andere plaatsen binnen en buiten het gebouw. Het gebruik van camera's en de eventuele vastlegging van beelden is gericht op de veiligheid van medewerkers van de SVB en de organisatie zelf. In uitzonderlijke gevallen kan de Directeur HR, Inkoop & Facilities met toestemming van de RvB, als er verdenkingen bestaan tegen een of meerdere werknemers en/of een of meer externen, onder voorwaarden gebruik maken van camera's die niet zichtbaar zijn.

Hoe meld je niet integer handelen en ongewenste omgangsvormen?

Iedereen is medeverantwoordelijk voor het correct omgaan met personen en middelen.

- Uitgangspunt is dan ook dat je de collega die niet integer handelt, aanspreekt op zijn gedrag.
- Als de collega zijn gedrag niet verandert dan ga je naar je direct leidinggevende en kaart je de situatie aan. Ook als het voor jou niet wenselijk of mogelijk is je collega eerst zelf aan te spreken, kun je je tot je direct leidinggevende wenden.
- Bij ongewenste omgangsvormen is het zeer goed mogelijk dat je de collega (tegen wie de melding is gericht) niet rechtsreeks wilt of kunt aanspreken op zijn gedrag, omdat je persoonlijk ernstig door deze collega bent gekwetst. Het is dan begrijpelijk dat je deze collega het liefst vermijdt. Je treedt dan in contact met je directe leidinggevende. Hij zal dan actie ondernemen.
- Het kan voorkomen dat het niet mogelijk of wenselijk is om de situatie bij je direct leidinggevende aan te kaarten. In dat geval kun je ook naar je naast hogere leidinggevende stappen, die actie zal ondernemen. De schending wordt in de “lijn” opgepakt.
- Als de situatie niet wordt aangepakt door je leidinggevenden, dan kun je melding doen bij de Commissie Integer Handelen. Ook als je denkt dat de impact van de (mogelijke) schending over meerdere SVB organisatieonderdelen merkbaar zal zijn, dan kun je je rechtstreeks wenden tot de Commissie Integer Handelen. De Commissie Integer Handelen zal als onafhankelijke commissie de melding in behandeling nemen en onderzoek verrichten naar het (vermoedelijke) incident. Als je geen mogelijkheid ziet om je tot je leidinggevende of je naast hogere leidinggevende te wenden, dan kun je ook rechtstreeks naar de Commissie Integer Handelen.

Wie kan je ondersteunen?

Daarnaast kun je te allen tijde in gesprek gaan met de vertrouwenspersoon, Bedrijfsmaatschappelijk werker of HR-adviseur. Meer informatie hierover vind je op pagina 14 of op intranet.

Meer informatie over de behandeling van een melding bij de Commissie Integer Handelen kun je vinden in het Reglement melding niet integer handelen op intranet.

Commissie Integer Handelen

T.a.v. Secretaris Commissie Integer Handelen
p/a Directie Juridische Zaken
Postbus 1100
1180BH Amstelveen

Hoe meld je misstanden; "klokkenluiden"

Het zogenaamde 'klokkenluiden' ontstaat als SVB-medewerkers informatie, waarover zij (uit hoofde van hun functie) beschikken, naar buiten brengen om zo ernstige misstanden binnen de SVB aan de kaak te stellen. Een misstand is een op redelijke gronden ontstaan vermoeden, voortvloeiend uit de kennis die de werknemer heeft opgedaan bij de werkgever, waarbij ook het maatschappelijke belang in het geding is. Het gaat dan om gevaarlijke, immorele of illegale praktijken.
Het maatschappelijk belang is bijvoorbeeld in het geding bij een zware schending van wettelijke voorschriften, waaronder strafbare feiten, verspilling van overheidsgeld, een gevaar voor aantasting van het milieu, de volksgezondheid of de veiligheid van personen. In principe gaat het hier om situaties die het niveau van een geval of enkele persoonlijke gevallen overstijgen, bijvoorbeeld vanwege de ernst van de situatie, de omvang of het structurele karakter ervan.

Op 1 juli 2016 is de Wet Huis voor klokkenluiders in werking getreden. Uitgangspunt is dat je een misstand eerst intern aan de orde stelt bij je (direct) leidinggevende of de commissie Integer Handelen.

Het verschil tussen misstanden en integriteitsschendingen is, dat bij integriteitsschendingen de normen en waarden van de organisatie (zoals neergelegd in de Gedragscode) worden geschonden, maar het maatschappelijk belang (nog) niet in het geding is. Bij misstanden is het maatschappelijk belang altijd in het geding.
Indien je wilt overgaan tot een externe melding, dan doe je dit aan de meest in aanmerking komende instantie, die effectief kan ingrijpen en waarbij de SVB zo min mogelijk schade lijdt als gevolg van het ingrijpen. Is er geen geschikt extern meldpunt, of weet je niet bij welke instantie je de melding kunt doen, dan kun je een externe melding doen bij de afdeling Onderzoek van het Huis voor Klokkenluiders: zie www.huisvoorklokkenluiders.nl

Voor het extern melden gelden de volgende uitgangspunten:
- met de bekendmaking is het maatschappelijk belang ernstig in het geding;
- je hebt de feiten eerst intern aan de orde gesteld, zo nodig op het hoogste niveau en dit heeft tot onvoldoende acties geleid, waardoor het maatschappelijk belang nog steeds ernstig in het geding is.
- het belang van externe bekendmaking in maatschappelijk opzicht is groter dan het belang van de SVB bij geheimhouding. Je maakt de feiten op een passende en evenredige wijze extern bekend. Je bent verplicht melding te maken aan de Commissie Integer Handelen, welke feiten je bekend hebt gemaakt en aan welke instantie(s).

De melder mag niet worden benadeeld in zijn positie als gevolg van de melding, als hij de SVB procedures die hiervoor gelden in acht heeft genomen. De melding wordt vertrouwelijk behandeld. De melder geniet bescherming.

De meldregeling Vermoeden van een misstand wordt geïntegreerd in het Reglement meldingen niet integer handelen en is te vinden op Intranet onder Gezond en veilig werken.

Huisregels

We verwachten van je dat je onderstaande huisregels opvolgt.

Clear desk

Binnen de SVB geldt een 'clear desk policy'. Dit betekent dat vertrouwelijke en/of geheime informatie voor derden niet toegankelijk is. Als de informatie is vastgelegd op een fysiek medium, bewaar je dit in een afgesloten ruimte en/of kast. Als de informatie is vastgelegd op digitale wijze, wordt deze bewaard op beveiligde plekken op het netwerk. Je moet de computer vergrendelen wanneer je de werkplek verlaat.

Media

Verzoeken van de media om informatie verwijs je onmiddellijk door naar de Directie Communicatie en Voorlichting.

Roken

Is alleen toegestaan op de daarvoor speciaal aangewezen gelegenheden binnen of buiten het SVB-kantoor. Dit geldt ook voor e-sigaretten.

Bezoekers

Bezoekers melden zich bij de receptie. Desgevraagd dienen zij zich te kunnen legitimeren. Tijdens hun bezoek, bij het betreden en bij het verlaten van het niet voor publiek toegankelijk gedeelte van de locatie moeten zij worden begeleid door een medewerker van de SVB. Ze dragen een bezoekerspas bij zich, die bij vertrek wordt ingeleverd.

BHV

Iedereen binnen de SVB volgt de aanwijzingen van de BHV bij ongevallen en calamiteiten stipt op. Bij calamiteiten van grotere omvang treedt het bedrijfsnoodplan in werking. Iedereen volgt de instructies die volgen uit het bedrijfsnoodplan op. Als het ontruimingssignaal klinkt moet je direct en beheerst het gebouw verlaten, en moeten de aanwijzingen van de BHV worden opgevolgd. Je bent als medewerker van de SVB verantwoordelijk voor je eigen bezoekers. Je zorgt ervoor dat je samen met hen het gebouw verlaat en bij hen blijft op de verzamelplaats. Je meldt je bij je leidinggevende, zodat vastgesteld kan worden dat je daadwerkelijk het gebouw hebt verlaten. Overwerk of andere vormen van aanwezigheid meld je altijd bij de daarvoor verantwoordelijke binnen de locatie.

Melding calamiteiten

Calamiteiten, ongevallen en/ of storingen meld je altijd.
Volg hierbij de instructies van de eigen locatie.

Over het algemeen geldt:

- calamiteiten (van fysieke aard zoals brand, rampen, etc.): **via het lokale alarmnummer** bij de beveiligingsorganisatie
- ongevallen (van fysieke aard zoals EHBO gevallen): **via het lokale alarmnummer** bij de beveiligingsorganisatie en/of de BHV
- niet ICT Storingen: bij HR, Inkoop & Facilities.
- ICT Storingen: bij de ICT Servicedesk (locatie Amstelveen).

Inwerkingtreding

Deze regeling treedt in de plaats van de voorgaande Gedragscode SVB.
Deze regeling treedt in werking op 15 september 2018.