Integriteitsverklaring

Naam:

Werkzaam bij de organisatie: **team/afdeling:**

Aard van de werkrelatie:

- uitzendkracht
- consultant
- stagiair
- schoonmaak/catering/onderhoudsbedrijven
- gedetacheerde
- overige externe medewerker die op projectbasis/opdracht wordt ingehuurd

Omschrijving werkzaamheden/opdracht:

Ondergetekende verklaart:

1. Integriteit

Ik gedraag mij integer, wat in ieder geval inhoudt dat ik mij houd aan de interne regels over integriteit van de organisatie. Bij twijfel raadpleeg ik mijn aanspreekpunt/contactpersoon binnen de organisatie, of de Vertrouwenspersoon Integriteit.

2. Geheimhouding

Ik verklaar geheim te houden, ook na beëindiging van mijn werkzaamheden, alle informatie waarvan ik kennis neem door mijn werkzaamheden bij bovengenoemde organisatie en waarvan ik weet of redelijkerwijs zou kunnen aannemen dat deze vertrouwelijk is. Persoonsgegevens, financiële gegevens, klantgegevens, aanbestedingsgegevens en contractgegevens beschouw ik in ieder geval als vertrouwelijk. Ik verstrek deze informatie niet aan anderen, ook niet binnen de organisatie, tenzij dit noodzakelijk is voor de uitoefening van mijn taak of dat ik daartoe wettelijk verplicht ben. Bij twijfel neem ik contact op met mijn aanspreekpunt/contactpersoon of de privacybeheerder binnen de organisatie.

3. Toegang tot gebouwen, apparatuur en kwetsbare ruimten

Ik gebruik de hulpmiddelen voor toegang tot locaties, apparatuur en ruimten van de organisatie uitsluitend voor het doel waarvoor deze aan mij ter beschikking zijn gesteld en uitsluitend gedurende de periode dat mijn werkzaamheden duren. Ik probeer niet om onbevoegd toegang te krijgen tot kwetsbare ruimten en locaties van de organisatie. Voor mij bestemde toegangsmiddelen behoud ik voor mijzelf en geef ik niet aan collega's of derden, tenzij daarover andere afspraken zijn gemaakt en dit past binnen de bedrijfsvoering.

Bij vermissing, ontvreemding, misbruik of ander onrechtmatig gebruik van de aan mij verstrekte toegangspas, sleutels, tags, toegangscodes, apparatuur of software stel ik de daartoe aangewezen personen binnen het organisatieonderdeel waar ik werkzaam ben onmiddellijk daarvan in kennis. Ik houd mij aan de regels die per locatie van de organisatie zijn gesteld ten aanzien van het ontvangen en begeleiden van bezoekers (zie toelichting).

4. Omgang informatie

Ik laat geen gegevens of informatie en/of de toegang daartoe onbeheerd achter, ook niet op mijn bureau, in de ruimte of (thuis)werkplek waar ik werk, waarvan ik weet of redelijkerwijs zou kunnen weten dat deze vertrouwelijk zijn. Ik houd mij op mijn (thuis)werkplek aan de regels voor de beveiliging van informatie. Als ik vermoed dat er een inbreuk wordt gemaakt op de informatieveiligheid dan doe ik daarvan een melding aan mijn leidinggevende.

Ik beperk de inzage en/of het gebruik van vertrouwelijke gegevens tot wat nodig is voor de vervulling van mijn werkzaamheden (Need-to-Know principe).

Documenten, e-mails, en overige zaken die niet voor mij bestemd zijn, zend ik onmiddellijk door aan het juiste adres of ik retourneer deze aan de afzender. Is het juiste adres noch de afzender bekend, dan vernietig ik ze (zie toelichting).

5. Omgang bedrijfsmiddelen

Ik ga zorgvuldig om met alle mij ter beschikking gestelde bedrijfsmiddelen, zowel op mijn werkplek als elders waar ik bedrijfsmiddelen gebruik. Ik houd mij aan de geldende regels voor e-mail- en internetgebruik en de huisregels van de organisatie. Ik laat geen waardevolle bedrijfsmiddelen onbeheerd achter op mijn werkplek of elders waar ik bedrijfsmiddelen gebruik. (zie toelichting).

6. Omgangsvormen

Ik houd mij aan correcte omgangsvormen en de geldende gedragscode van de organisatie.

Ondergetekende verklaart verder:

- in kennis te zijn gesteld van de inhoud van dit formulier door de organisatie;
- zich te zullen houden aan alle in dit formulier genoemde (spel)regels;
- bekend te zijn met het feit, dat het handelen in strijd met de gedragscode kan leiden tot maatregelen;
- bekend te zijn met de verplichting melding te doen van elke schending van de geheimhoudingsplicht bij zijn aanspreekpunt/contactpersoon binnen de organisatie;
- de gedragscode van de organisatie te hebben ontvangen en kennis te hebben genomen van de inhoud van de code.

Plaats: Datum:

Naam medewerker:

Handtekening medewerker:

Toelichting bij integriteitsverklaring

Algemeen
Elke externe medewerker ontvangt deze integriteitsverklaring voor de start van zijn werkzaamheden bij de organisatie. Na het doornemen van de verklaring en deze toelichting moet de verklaring ondertekend worden. Een overheidsorganisatie is wettelijk verplicht hiervoor te zorgen. Wanneer geweigerd wordt de verklaring te tekenen kunnen de werkzaamheden niet worden gestart.

Gegevensverwerking (dit is ook het raadplegen van gegevens in SUWInet of de Basisregistratie personen (BRP), direct of via een andere applicatie) is noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak en in het belang van de betrokken burger. Als de gegevens niet nodig zijn, dan mogen ze ook niet worden geraadpleegd. Dit betekent ook dat van een burger/klant niet meer gegevens worden opgevraagd, dan voor het werk nodig is. We noemen dit ook wel “Need-to-Know”.

In de meeste applicaties is het toegangsbeheer per groep geregeld. Een medewerker heeft dus dezelfde rechten als zijn collega’s, maar heeft niet het recht om gegevens te bekijken van een klant van een collega. Als niet kan worden uitgelegd waarom gegevens zijn opgevraagd, is waarschijnlijk gehandeld in strijd met de bepalingen uit o.a. de Wet bescherming persoonsgegevens.
Alle opvragingen worden geregistreerd (logging) en regelmatig gecontroleerd! Dit is een wettelijke verplichting.

Geheimhouding betekent ook dat deze informatie niet met anderen wordt gedeeld, behalve als daar een wettelijk verplicht toe is (o.a. samenwerking Sociaal Domein). Concreet komt dit neer op een Clean Desk Policy (geen vertrouwelijke informatie open en bloot laten liggen, ook niet op het scherm van de computer) en niet over klanten/burgers praten als dit niet nodig is. Moet dat wel, zorg er dan voor dat anderen niet kunnen meeluisteren. Is dat niet mogelijk, doe het dan zo dat niet herkenbaar is over wie (geen namen of adressen noemen) het gaat.

De wetgever neemt geheimhouding serieus. In artikel 272 van het Wetboek van Strafrecht staat: “Hij die enig geheim waarvan hij weet of redelijkerwijs moet vermoeden dat hij uit hoofde van ambt, beroep of wettelijk voorschrift dan wel van vroeger ambt of beroep verplicht is het te bewaren, opzettelijk schendt, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie (per 1 januari 2016: € 20.500,-). In minder ernstige gevallen neemt de werkgever disciplinaire maatregelen, die kunnen variëren van een waarschuwing tot ontslag.

Ad 3. Toegang tot gebouwen, apparatuur en kwetsbare ruimten
Met locatie wordt bedoeld elk gebouw waarin een onderdeel van de organisatie is gevestigd, of een plaats waar medewerkers van de organisatie werkzaam zijn, dus ook bedrijfsterreinen, kunstwerken, vervoermiddelen, etc.

Toegangsmiddelen zijn bijvoorbeeld toegangspassen, sleutels, tags, toegangscodes, passwords, apparatuur en software.

Voorbeelden van kwetsbare ruimten zijn: computer- en netwerkruimten, patchkasten, ruimten met communicatieapparatuur zoals telefooncentrales, archiefruimten, ruimten met toegang tot bedrijfsvoeringgegevens, ruimten waarin zich kluizen bevinden, werkplaatsen/laboratoria waar kostbare apparatuur aanwezig is.

Ad 4. Omgang informatie
In ieder geval worden als vertrouwelijk beschouwd: persoonsgegevens, financiële gegevens, klantgegevens, aanbestedingsgegevens en contractgegevens.

Voorbeelden van mogelijke beveiligingsmaatregelen zijn: clean desk, afsluiten kasten, aanzetten schermbeveiliging tijdens afwezigheid, regelmatig wijzigen van wachtwoorden, niet uitlenen van apparatuur of gegevensdragers aan derden en het niet periodiek maken van reservekopieën van informatie op laptop of computer op de thuiswerkplek.

Ad 5. Omgang bedrijfsmiddelen
Voorbeelden van bedrijfsmiddelen zijn: computers, (mobiele) telefoons, kantoorbehoeften, laptops, beamers, vervoermiddelen zoals dienstauto of dienstfiets.

Voorbeelden van ongewenst gebruik van inter-/intranet en e-mail zijn het surfen naar dubieuze websites, het openen van e-mail van totaal onbekende afzenders dan wel e-mail met een vreemde bijlage, het downloaden van muziekbestanden of software zonder licentie, etc.