Belastingsamenwerking
gemeenten & hoogheemraadschap Utrecht

# Strategisch Informatiebeveiligingsbeleid

Beter veilig dan sorry!

Datum: 22-09-2020
Versie: 0.9
Status: concept
Opsteller: CISO Sam Lee, s.lee@bghu.nl

# Versiebeheer

Deze beleidsnota beschrijft het strategische informatiebeveiligingsbeleid voor de jaren 2021 t/m 2024 en vervangt het vastgestelde BghU informatiebeleidsplan van voorgaande jaren.

| Versie | Datum | Door | Wijzigingen |
|---|---|---|---|
| **0.1** | 05-11-2019 | Sam Lee | Eerste conceptversie |
| **0.2** | 06-05-2020 | Sam Lee | Bijlagen toegevoegd |
| **0.3** | 25-05-2020 | Sam Lee/Richard Dalebout | Opmerkingen Bastiaan Vos, Richard Dalebout en HR verwerkt |
| **0.4** | 29-05-2020 | Ronald Rosdorff | Opmerkingen Ambitie verwerkt |
| **0.5** | 11-06-2020 | Bastiaan Vos | 3.5 uitvoering Financiën toegevoegd |
| **0.6** | 17-08-2020 | Sam Lee/Richard Dalebout | Opmerkingen Richard Dalebout verwerkt |
| **0.7** | 23-08-2020 | Sam Lee | Opmerkingen Marieke Vrisou van Eck verwerkt |
| **0.8** | 27-08-2020 | Sam Lee | 3.8 Incident afhandeling/ crisis beheersing aangepast |
| **0.9** | 22-09-2020 | Sam Lee | Opmerkingen RegieOverleg met onze deelnemers verwerkt. |
| **1.0** | 28-09-2020 | | definitief |

# Inhoudsopgave

# Relaties met andere documenten

Deze Strategische Baseline Informatiebeveiligingsbeleid maakt onderdeel uit van de informatiebeveiliging documenten set (in feite het kader rondom informatiebeveiliging, de set aan documenten is het middel). Deze bestaat naast het Strategisch beleid en het Tactisch beleid verder uit een informatiebeleidsplan en procedures.

# Samenvatting

Deze beleidsnota beschrijft het **BghU informatiebeveiligingsbeleid.** Met dit beleid zet de BghU een volgende stap om de beveiliging van informatie te verbeteren, zodat een betrouwbare dienstverlening aan onze klanten mogelijk blijft. Dit beleid wordt uitgewerkt in tactische plannen en geeft richting aan de te treffen operationele beveiligingsmaatregelen.

**Wat is informatiebeveiliging?**
Onder informatiebeveiliging wordt verstaan het inrichten van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening te verzekeren. Kernpunten daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid van (persoons)gegevens.

**Voor wie is het beleid van toepassing?**
Het informatiebeveiligingsbeleid geldt voor alle processen en medewerkers (tijdelijke en structurele) van de BghU. Het beperkt zich niet alleen tot de ICT maar heeft ook betrekking op de gehele BghU organisatie, deelnemende gemeenten, deelnemende waterschap, klanten, gasten, bezoekers en externe relaties.

**Waarom is beleid belangrijk?**
Beleid op het gebied van de beveiliging van informatie is belangrijk omdat klanten en bedrijven zich steeds meer zorgen maken over de bescherming van hun gegevens en hun privacy. Door technische ontwikkelingen neemt de afhankelijkheid van de informatie toe en daarmee ook de noodzaak de informatiebeveiliging op een adequaat niveau te brengen. Ook ontstaan steeds meer risico's voor de informatieveiligheid door toename van de cybercriminaliteit.

**Hoe wordt invulling gegeven aan de informatiebeveiliging?**
De basis voor de inrichting van de informatiebeveiliging is het normenkader Baseline Informatiebeveiliging Overheid (BIO). De BghU heeft de plicht om ieder jaar verantwoording af te leggen over informatiebeveiliging aan haar deelnemers. De BghU zal zorgen voor een veilige cultuur, het uitvoeren van risicomanagement voor informatieveiligheid en zal zorgen voor informatiebeveiliging in de samenwerking met andere partijen.
Het bestuur, de directeur en de managers spelen een belangrijke rol bij het uitvoeren van dit beleid. Het management maakt een inschatting van de risico's die de BghU loopt. Op basis hiervan stelt het management dit beleid voor informatiebeveiliging op, draagt dit uit naar de rest van de organisatie en ondersteunt en bewaakt de uitvoering ervan middels uitvoering van plannen en maatregelen. Informatiebeveiliging is onderdeel van de PDCA-rapportagecyclus.

**Wie is verantwoordelijk?**
Het bestuur is eindverantwoordelijk voor de informatiebeveiliging. De daadwerkelijke uitvoering van de informatiebeveiliging is een verantwoordelijkheid van directeur en management. De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de BghU bij het bewaken en verhogen van de informatieveiligheid.

**Wat is onze rol voor informatiebeveiliging?**
Alle medewerkers van de BghU dragen verantwoordelijkheid voor de veiligheid van de activiteiten en de informatie die behoren tot hun functie en moeten zorgvuldig omgaan met informatie. De medewerkers worden daarom regelmatig getraind in het gebruik van informatiebeveiligingsprocedures. Iedere medewerker is verplicht om een (mogelijk) informatiebeveiligingsincident direct te melden bij de CISO of de manager.

# 1. Scope

Deze beleidsnota beschrijft het strategische BghU informatiebeveiligingsbeleid voor de jaren 2021 t/m 2024 en vervangt het vastgestelde BghU informatiebeleidsplan van voorgaande jaren.

Deze nota is opgesteld door de CISO, waarbij gebruik is gemaakt van de adviezen en het format Informatiebeveiligingsbeleid zoals beschikbaar gesteld door de Informatiebeveiligingsdienst (IBD). De basis voor dit strategische beleid is de NEN-ISO/IEC 27001/2:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (BIO). Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerp specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau. Informatiebeveiliging is expliciet opgenomen binnen de Nederlandse Overheid Referentie Architectuur (NORA). Dit is het overheidsbrede architectuur raamwerk.

Met dit strategische informatiebeveiligingsbeleid zet de BghU een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de organisatie te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn.

## 1.1 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategische beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels (‘tactisch handboek’). In het jaarlijks uit te brengen Informatiebeveiligingsplan dat wordt opgesteld door de CISO worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de managers, het dreigingsbeeld van de IBD, ervaringen met incidenten en de uitkomsten van diverse audits. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

## 1.2 Wat is informatiebeveiliging?

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen.
Kernpunten daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid van persoonsgegevens en andere informatie.
Informatiebeveiliging heeft betrekking op:

- Alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, etc.);
- Alle mogelijke informatiedragers (papier, schijven, DVD, foto, video, etc.);
- Informatiebeveiliging is van toepassing op gegevens, gegevensdragers en vanuit die gegevens de betreffende informatie.

Het informatiebeveiligingsbeleid geldt voor alle processen van de BghU en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op de leden van het bestuur, de directeur, alle medewerkers van de BghU, deelnemende gemeenten (Bunnik, De Bilt, Houten, Lopik, Nieuwegein, Stichtse Vecht, Utrecht, Utrechtse Heuvelrug, Zeist), deelnemende waterschap (Hoogheemraadschap De Stichtse Rijnlanden), klanten, gasten, bezoekers en externe relaties.

## 1.3 Ambitie en visie van op het gebied van informatieveiligheid

In deze beleidsnota worden de visie en ambities van de BghU weergegeven op het thema informatiebeveiliging.

### 1.3.1 Visie

De missie van de BghU luidt als volgt:
De BghU heft en int lokale belastingen namens haar deelnemers, beheert de authentieke basisregistratie WOZ en verzorgt het product waarderen. De BghU voert deze taken uit voor haar deelnemers, zijnde gemeenten en het waterschap. Dit doet de BghU zo efficiënt mogelijk en op een zorgvuldige en pragmatische wijze, gericht op tijdigheid en volledigheid. De BghU is een uitvoerende en dienstverlenende organisatie die niet alleen op basis van bedrijfseconomische principes wordt geleid, maar ook oog heeft voor de belangen van de belastingbetaler binnen ons beheersgebied. De BghU vindt het belangrijk dat de belastingbetaler zich begrepen voelt en dat de BghU naar een passende oplossing zoekt (standaard versus maatwerk), dit alles in het licht van excellente dienstverlening.

Samengevat komt het erop neer dat de BghU efficiënt en dus slank en slim moet zijn ingericht. Dienstverlening op basis van bedrijfseconomische en maatschappelijke principes is alleen mogelijk met behulp van procesoptimalisatie en digitalisering. Investering in kennis en resultaatbewustzijn van medewerkers is noodzakelijk.

Informatie is één van de belangrijkste bedrijfsmiddelen van de BghU. Toegankelijke en betrouwbare gegevens en bescherming van waardevolle en persoonlijke informatie zijn van groot belang voor de inwoner, de bedrijven en de instellingen in het beheersgebied van de BghU. Beschikbare, juiste en volledige informatie is noodzakelijk voor het goed functioneren en leveren van excellente dienstverlening van de BghU. Dit vormt de basis voor het beschermen van rechten van klanten en bedrijven.
Dit vereist binnen de BghU een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij betrokken. Verantwoord en bewust gedrag van medewerkers is essentieel om informatieveiligheid te bereiken en te behouden. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de bedrijfsvoering maar ook leiden tot imagoschade. Ernstige incidenten hebben mogelijk negatieve gevolgen voor burgers, bedrijven, partners en de eigen organisatie met waarschijnlijk ook politieke consequenties. Informatieveiligheid is daarom van groot belang. Informatiebeveiliging (IB) is het proces dat dit belang dient.

De BghU ziet dat door maatschappelijke ontwikkelingen steeds hogere eisen worden gesteld aan de digitale volwassenheid en informatiebeveiliging van de organisatie:

- Als gevolg van de verdergaande digitalisering maken klanten en bedrijven zich steeds meer zorgen over de bescherming van hun gegevens en hun privacy;
- Door technische ontwikkelingen neemt de afhankelijkheid van de informatie toe en daarmee ook de noodzaak om de integriteit, vertrouwelijkheid en continuïteit van de informatie zeker te stellen;
- Door toename van de cyber-dreigingen nemen de risico's toe: onder meer privacy schendingen door een datalek, economische schade door het uitlekken van vertrouwelijke plannen en fysieke schade door storingen in systemen in de openbare ruimte, informatiediefstal en ondermijning van de processen (zie ook Dreigingsbeeld Informatiebeveiliging Nederlandse gemeenten 2019/2020).

### 1.3.2 Ambitie

De BghU spreekt de ambitie uit om intensief samen te werken op het gebied van informatiebeveiliging (met regionale belastingkantoren, gemeentelijke afnemers en het waterschap) en de gezamenlijke informatiebeveiliging naar een hoger volwassenheidsniveau te brengen. De organisatie wil hierbij aantoonbaar de juiste beheersingsmaatregelen treffen ('in control' zijn) en de noodzakelijke verbeteringen van de beveiligingsmaatregelen volgens een concrete planning uitvoeren ('plan-do-check-act' - cyclus).

De BghU dient te voldoen aan de landelijke normen, zoals de Baseline Informatiebeveiliging Overheid (BIO). Daarbij zal de BghU goede bestuurlijke principes van informatiebeveiliging toepassen, zoals het bevorderen van een veilige cultuur, toepassen van risicomanagement voor informatieveiligheid, aandacht voor informatiebeveiliging in de (keten)samenwerking en controle en evaluatie door het bestuur (zie ook 2.2.2).

De BIO bestaat uit een baseline met verschillende niveaus van beveiligen (basisbeveiligingsniveau 's (BBN)). De BghU zal periodiek de processen en IT-systemen toetsen aan de hand van het BIO-BBN-toetsingskader, Het BIO-BBN- toetsingskader bepaalt per proces of de BghU dient te voldoen aan BBN 1 of BBN 2.

De implementatie van de noodzakelijke beheersingsmaatregelen gebeurt stapsgewijs en vindt plaats op verschillende volwassenheidsniveaus. De ambitie van de BghU is de komende jaren te groeien van de huidige volwassenheidsniveaus '1' (ad/hoc proces) resp. '2' (herhaalbaar proces maar intuïtief) naar niveau '3' (gedefinieerd proces) eind 2021.
Toekomstige niveaus zijn '4' (bestuurd en meetbaar proces) en '5' (geoptimaliseerd proces), start begin 2022 en gereed eind 2024: op basis van jaarlijkse voortgangsevaluatie zo nodig planning naar voren of achteren bijstellen.

# 2. Strategisch beleid

## 2.1 Doel

Het doel van deze beleidsnota is het presenteren van het strategische informatiebeveiligingsbeleid voor de jaren 2021 tot en met 2024. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan dat wordt opgesteld door de CISO.

## 2.2 Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van het informatiebeveiligingsbeleid van de BghU zijn in onderstaande paragrafen beschreven.

### 2.2.1 De BIO

De Baseline Informatiebeveiliging Overheid (BIO) is vanaf 1-1-2020 het nieuwe normenkader voor de gehele overheid, vervangt de BIG (gemeenten) en de BIWA (waterschappen). Zie Bijlage-C-BghU-70463-rapport-bio-versie-104.pdf. De werkwijze van deze BIO is meer gericht op risicomanagement dan de oude Baseline Informatiebeveiliging voor Gemeenten (BIG). Dat wil zeggen dat de managers nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd is in termen van beschikbaarheid, integriteit en vertrouwelijkheid. Door hetzelfde normenkader voor de overheid te hanteren wordt de samenwerking tussen de overheden gestimuleerd en vereenvoudigd. De Informatiebeveiligingsdienst (IBD) ondersteunt bij de implementatie van de BIO middels diverse producten en generieke dienstverlening. Doelgroepen hiervoor zijn:

- Nederlandse gemeenten;
- ICT samenwerkingsverbanden van gemeenten;
- Intergemeentelijke sociale diensten;
- Gemeentelijke belastingsamenwerkingen;
- VNG.

### 2.2.2 De 10 bestuurlijke principes voor informatiebeveiliging

De 10 principes voor informatiebeveiliging (opgesteld door de VNG) zijn een bestuurlijke aanvulling op het normenkader [1] BIO en gaan over de waarden die de bestuurder zichzelf oplegt. Zie Bijlage-B-BghU-De-10-bestuurlijke-principes-voor-Informatiebeveiliging_20190109.pdf

De principes zijn als volgt:

1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

*[1] Deze principes zijn gelijk met de BIO van kracht, zie besluitvorming Informatiebeveiligingsdienst (IBD) en Verenigde Nederlandse Gemeenten (VNG)*

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de organisatie. Deze principes ondersteunen de bestuurder bij het bepalen van de kaders voor een goed risicomanagement (de organisatie voert uit). Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers, partners van de BghU en de dienstverlening aan deze partijen. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel en van belang dat het bestuur de kaders vaststelt.

### 2.2.3 Dreigingsbeeld Informatiebeveiliging Nederlandse gemeenten

Het Dreigingsbeeld Informatiebeveiliging Nederlandse gemeenten 2019/2020 (VNG) geeft een actueel zicht op de beveiligingsincidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is daarmee het ideale document om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging. Enkele aandachtspunten uit het dreigingsbeeld informatiebeveiliging uit de versie 2019/2020.

Interne beveiligingsincidenten en factoren uit het verleden:

- Imagoprobleem informatiebeveiliging;
- Risico's niet integraal in beeld;
- Basis niet op orde;
- Te weinig mensen (te veel werk en te weinig gekwalificeerde specialisten);
- De complexiteit neemt toe

Externe beveiligingsincidenten en factoren uit het verleden:

- Verkrijging en openbaarmaking van informatie;
- Identiteitsfraude;
- Verstoring ICT;
- Manipulatie van data;
- Spionage;
- Overname en misbruik ICT;
- Bewust beschadigen imago

De belangrijkste trends en ontwikkelingen voor informatieveiligheid zijn:

- Aandacht voor privacy;
- Baseline Informatiebeveiliging Overheid;
- Internet of things (IoT)en smart society;
- Kunstmatige intelligentie (AI);
- Common Ground

De prioriteiten voor organisaties:
Om de belangrijkste risico's te beheersen is een combinatie van technische en organisatorische maatregelen noodzakelijk. De IBD adviseert gemeenten voor 2019/2020 de volgende prioriteiten te stellen:

- Zet informatiebeveiliging op de agenda van het college en zorg dat lijnmanagers verantwoordelijkheid kunnen nemen;
- Breng de basis op orde;
- Versterk de menselijke schakel;
- Versterk de positie van de CISO;
- Verbeter het inzicht in de risico's van nieuwe technologieën

Het dreigingsbeeld is één van de producten die door de Informatiebeveiligingsdienst (IBD) worden geleverd ter ondersteunen van de gemeentelijke organisaties.

### 2.2.4 Informatie uit lokale incidenten en inbreuken op de beveiliging

De BghU kent naast het hierboven genoemde dreigingsbeeld een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid en voor het treffen van beveiligingsmaatregelen.
Een voorbeeld:

- De manier waarop met verdachte (phishing) mails wordt omgegaan of gemeld gebeurt nog niet op uniforme wijze. Dit betekent meer aandacht voor dit onderwerp zodat gebruikers er bewuster naar kunnen handelen.

## 2.3 Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2017. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2017 genomen.
Voor de ondersteuning van de overheidsorganisaties bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[2] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide Nen-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen. Ook zullen praktische operationele handreikingen worden uitgebracht, zoals een handleiding voor het uitvoeren van risicoanalyses en voor het opstellen van een beveiligingsplan.
De inhoud en structuur van dit informatiebeveiligingsbeleid zijn afgestemd op die van de NEN-ISO en de BIO. Ook het Informatiebeveiligingsplan zal deze structuur volgen.

## 2.4 Plaats van het strategisch beleid

Het strategische informatiebeveiligingsbeleid van de BghU wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau.
Deze nota beschrijft op strategisch niveau het informatiebeveiligingsbeleid van de BghU. Dit beleid zal worden vertaald in tactische en operationele richtlijnen en maatregelen ('tactisch handboek'). De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks bij te stellen informatiebeveiligingsplan.

## 2.5 Scope informatiebeveiliging

De scope van dit beleid omvat alle BghU processen, onderliggende informatiesystemen, informatie en gegevens van de BghU en de (geautomatiseerde) uitwisseling van gegevens met externe partijen (bijvoorbeeld afnemers (gemeenten en waterschappen) en WOZ-bureaus), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Dit strategische BghU informatiebeveiligingsbeleid is een algemene basis en dekt tevens algemene aanvullende beveiligingseisen uit wetgeving af zoals bijvoorbeeld, BAG, BRP, Kadaster, NHR en WOZ. Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld DigiD). Deze worden in aanvullende documenten geformuleerd.
Bewust wordt in het strategisch beleid geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

[2] *De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.*

Wanneer gegevens zijn te herleiden naar een specifiek persoon (klanten en medewerker) dan is er sprake van persoonsgegevens en moet er rekening worden gehouden met de privacy vereisten. Hoewel privacybescherming binnen de BghU een eigen aanpak kent is het belangrijk vast te stellen dat er een overlap bestaat tussen privacy/data-protectie en informatiebeveiliging en dat nauwe samenwerking tussen beide werkvelden noodzakelijk is en in de praktijk ook plaatsvindt. Goede informatiebeveiliging is een randvoorwaarde voor het beschermen van de privacy van klanten en medewerkers.

## 2.6 Uitgangspunten

Het bestuur, de directeur en de managers van de BghU spelen een cruciale rol bij het vormgeven en uitvoeren van dit strategisch informatiebeveiligingsbeleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de BghU heeft, de risico's die het 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 gehele management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een informatiebeveiligingsbeleid van en voor de hele organisatie. 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 van de BghU en de relevante landelijke en Europese wet- en regelgeving.

### 2.6.1 Strategische doelen

De strategische doelen van het informatiebeveiligingsbeleid zijn:

- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van kritieke bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van klanten en medewerkers.
- Het waarborgen van de naleving van dit beleid.

### 2.6.2 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

- De borging van de informatievoorziening is van vitaal belang voor de taakuitvoering door de BghU. Het bestuur is eindverantwoordelijk voor de informatiebeveiliging.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het management. Alle processen, informatiebronnen en systemen in gebruik door de BghU hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. Jaarlijks wordt een informatiebeveiligingsplan opgesteld gebaseerd op:
    - De periodieke risicoanalyse;
    - De uitkomsten van de jaarlijkse Audits;
    - Het Dreigingsbeeld Informatiebeveiliging Nederlandse gemeenten (IBD);
    - De door de managers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn;
    - Leerpunten vanuit de informatiebeveiligingsincidenten die binnen de organisatie(s) hebben plaatsgevonden.
- In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatie breed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
- Bij ingrijpende wijzigingen kan het noodzakelijk zijn tussentijds het beleidsplan te wijzigen. Deze wijziging wordt dan aan het dagelijks bestuur voorgelegd
- Informatiebeveiliging is een continu verbeterproces. ‘Plan, do, check en act’ vormen samen het managementsysteem van informatiebeveiliging.
- De BghU stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

### 2.6.3 Invulling van de uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

| Onderwerp | Wie | Termijn |
|---|---|---|
| Vaststellen strategisch informatiebeveiligingsbeleid | Bestuur | 4 jaar |
| Vaststellen van het informatiebeveiligingsplan | Directie/MT | jaarlijks |
| Het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op het strategisch informatiebeveiligingsbeleid | Directie/MT | jaarlijks |
| Informatie opvragen bij de managers en erop toezien dat de managers adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt. | Directie | Maandelijks |

| Onderwerp | Wie | Termijn |
|---|---|---|
| Zorgen voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn. Hoewel de basiskernregistraties (zoals WOZ, BRP, BAG) en toekomstige basisregistraties belangrijk zijn in het kader van informatiebeveiliging, krijgen zij niet meer of minder voorrang dan andere (primaire) processen binnen de BghU. Het samenspel en balans van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de BghU en het behalen van de doelen die zijn gesteld. | Managers | continu |
| Managers dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben. | Managers | continu |
| Uitvoeren van QuickScans informatiebeveiliging op basis van de BIO om risico-afwegingen te kunnen maken.<br>De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. | Managers | continu |
| Het ondersteunen en adviseren vanuit een onafhankelijke positie van de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening. | CISO/FG | continu |
| Adviseren met betrekking tot beveiligingsmaatregelen en privacy. | CISO/FG | continu |
| Rapporteren aan de directeur en MT (voorafgaand aan de planning & control gesprekken). | CISO/FG | 2x per jaar |
| Het ontwikkelen het personeelsbeleid in relatie tot informatiebeveiliging en het ondersteunen en adviseren van de directie en managers bij de uitvoering hiervan. | HR | continu |
| Medewerkers worden getraind in het gebruik van informatiebeveiligingsprocedures. | Medewerkers | continu |
| Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie. | Medewerkers | continu |
| Medewerkers dragen verantwoordelijkheid voor de veiligheid van de activiteiten en de informatie die behoren tot hun functie. Zij betrachten zorgvuldigheid bij het omgaan met informatie en privacy. | Medewerkers | continu |

| Onderwerp | Wie | Termijn |
|---|---|---|
| Tijdens planning & control-gesprekken dient er aandacht te zijn voor de informatiebeveiliging n.a.v. de rapportage van de CISO. De onderwerpen die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen. | Controller | continu |
| Zorgen voor de interne controle op naleving van het informatiebeveiligingsbeleid, de realisatie van de maatregelen en de afhandeling van beveiligingsincidenten. | Controller | continu |
| De leveranciers vormen een belangrijke schakel in de keten voor het waarborgen van de veiligheid van de omgeving (Cloudomgeving en applicaties). | Leveranciers | continu |
| De IBD heeft inzicht in de belangrijkste dreigingen op het gebied van beveiliging. Binnen de organisatie zijn de algemene contactpersoon informatiebeveiliging (ACIB) en de vertrouwde contactpersoon informatiebeveiliging (VCIB) aanspreekpunt voor de contacten met de IBD. | ACIB/VCIB | continu |

### 2.6.4 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

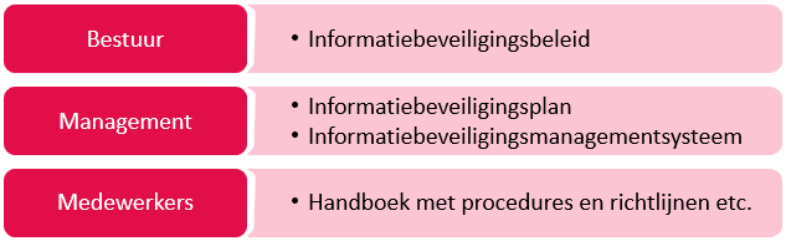
- De beveiliging van informatie maakt deel uit van afspraken met ketenpartners en is onderdeel van ons inkoopbeleid.
- Kennis en bewustzijn van informatiebeveiliging bij medewerkers en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Voldoende technische middelen om de controles te ondersteunen.
- Voldoende budget om de kennis en het bewustzijn op peil te houden.

# 3. Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD). In dit model zijn de managers verantwoordelijk voor de eigen processen. De tweede lijn (CISO, FG) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden voor adviezen tot verbetering.

## 3.1 Hoe is informatiebeveiliging geborgd?

Om het informatiebeveiligingsbeleid op een efficiënte en effectieve wijze te beheren, zijn de bijbehorende normen en maatregelen geregistreerd in een 'Informatiebeveiligings-managementsysteem' (ISMS). Het ISMS is een integraal kwaliteitssysteem voor informatiebeveiliging conform ISO 27002:2017 en is samen met het tactisch beleid vastgelegd in het informatiebeveiligingsplan (IBP) BghU. Het IBP is, samen met de handboeken met operationele procedures, onderdeel van het managementsysteem van de BghU. Schematisch weergegeven:




Figuur 1. Schematisch weergave borging informatiebeveiliging

## 3.2 Aansturing: directeur

De directeur zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een managers. De directeur zorgt dat de managers zich verantwoorden over de beveiliging van de informatie die onder hen berust. De directeur zorgt dat de eindverantwoordelijke bestuurders gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het bestuur zich ook verantwoorden naar de overige deelnemers.

De directeur stelt het gewenste niveau van continuïteit en vertrouwelijkheid van gegevens vast. De directeur draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO en FG van de BghU. De directeur autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt in de deelnemende organisaties gezien als een integraal onderdeel van risicomanagement.

## 3.3 Uitvoering: managers

Informatiebeveiliging valt onder de verantwoordelijkheden van alle managers.
Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. De managers rapporteren aan de directeur over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp Informatiebeveiliging te bespreken in het bedrijfsvoeringsoverleg. Voorbereiding en coördinatie van het overleg ligt bij de CISO en FG.

Taken van het managers in het kader van informatiebeveiliging zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het uitvoeren van lijncontroles op het gebied van informatiebeveiliging in het kader van integraal management.
- Het binnen de eigen afdeling uitdragen van het beveiligingsbeleid, de daaraan gerelateerde procedures.
- Informeren medewerkers over geheimhouding, integriteit en informatiebeveiliging.
- Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

## 3.4 Uitvoering: HR

Arbeidsvoorwaardelijke zaken valt onder de verantwoordelijkheden van de manager.
Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit HR.

Taken van HR in het kader van informatiebeveiliging zijn:

- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het verduurzamen van de relatie tussen personeelsbeleid en informatiebeveiliging.
- Het leveren van input bij het opstellen van gedragsregels met betrekking tot het veilig omgaan met informatie.
- Informeren nieuwe medewerkers bij arbeidsvoorwaardengesprek over geheimhouding, integriteit en informatiebeveiliging.
- Jaarlijkse controle middels steekproef op toegangsrechten en laten vervallen van rechten van ex-medewerkers.
- Het ondersteunen en adviseren van de directie, managers en CISO m.b.t. het bewustwordingsproces.

## 3.5 Uitvoering: financiën

Er zijn geen extra kosten verbonden aan het aanscherpen van de ambitie in het kader van informatiebeveiliging. De huidige inzet van de CISO en eventuele bewustwordingstrajecten worden gedekt vanuit de reguliere materiële en formatiebudgetten. Indien nog extra budget nodig blijkt dan wordt dit geraamd in het jaarlijks op te stellen afdelingsplan en/of het beveiligingsplan.

## 3.6 Controle en verantwoording

De directeur zal volgens de 10 principes voor informatiebeveiliging (zie 2.2.2) richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.

De directeur is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan het bestuur. De directeur rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid. Dit komt jaarlijks terug als rapportage in de jaarstukken BghU.
De (interne) auditors zijn verantwoordelijk voor de interne controle op naleving van het informatiebeveiligingsbeleid, de realisatie van de maatregelen en de afhandeling van beveiligingsincidenten.

## 3.7 Overleg

De volgende overlegstructuren zijn minimaal aanwezig:

- Overleg tussen directeur, MT, Business controller, CISO en FG: iedere 3 maanden;
- Overleg tussen informatiemanager, Business controller, CISO en FG: iedere 1 maand
- Overleg tussen de CISO en FG: wekelijks.
- Overleg tussen CISO en FG en vertegenwoordigers van uit procesteams: maandelijks
- Informatiebeveiligingsorganisatie binnen deelnemende organisaties (CISO): iedere 12 maanden; (samen met gemeentelijke vertegenwoordiging)
- Informatiebeveiligingsorganisatie binnen kernteam belastingorganisaties (CISO, FG): iedere 3 maanden;

## 3.8 Incident afhandeling/ crisis beheersing

Alle medewerkers zijn verplicht om (vermoeden van) (mogelijke) een informatiebeveiligingsincident direct te melden bij de CISO, FG of managers.

In geval van een informatiebeveiligingsincident of calamiteit met betrekking tot de beschikbaarheid, integriteit en/of vertrouwelijkheid van de BghU processen, komt een crisisteam informatiebeveiliging samen. De CISO bepaalt aan de hand van de situatie wanneer het team bij elkaar komt. Het team bestaat uit de CISO, betreffende managers, de directeur, informatiemanager, relevante interne of externe experts, en een lid voor de communicatie.

Voor de afhandeling van een informatiebeveiligingscalamiteit of - crisis worden beschikbare procedures en/of crisisplannen toegepast.

Als een incident de gegevens van een deelnemende organisatie raakt, dan zal de CISO van de betreffende organisatie geïnformeerd worden. Afhankelijk van de ernst van het incident wordt ook het bestuur van de BghU in de communicatie betrokken.
Jaarlijks zal aan het bestuur gerapporteerd worden over de aard, soort en het aantal incidenten.

Vastgesteld op: [datum] [plaats] het bestuur,

Vastgesteld op: [datum][plaats] het bestuur,

[Ondertekening]

# Bijlage
# Relevante begrippen en afkortingen

**ACIB:** Algemene Contactpersoon Informatiebeveiliging
**Audit:** Vastlegging van de complete keten van opeenvolgende wijzigingen op een object in een bepaalde periode.
**AVG:** uitvoeringswet Algemene Verordening Gegevensbescherming
**BAG:** Basisregistratie Adressen en Gebouwen
**BBN:** Basis Beveiligings Niveau
**Bedrijfsmiddel:** Elk middel waarmee bedrijfsgegevens kunnen worden opgeslagen en/of verwerkt en waarmee toegang tot gebouwen, ruimten of ICT-voorzieningen kan worden verkregen: een bedrijfsproces, een gedefinieerde groep activiteiten, een gebouw, een apparaat, een ICT voorziening of een gedefinieerde groep gegevens.
**Beschikbaarheid:** De waarborg dat vanuit hun functie geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen.
**Beveiliging:** Het brede begrip van informatiebeveiliging, inclusief fysieke beveiliging, Business Continuïty Management (BCM), ofwel beschikbaarheid van bedrijfsprocessen en integriteit.
**Beveiligingsincident:** Het manifest worden van een beveiligingsrisico (dreiging, oorzaak) als gevolg van een overtreding van een beveiligingsregel, bijv. onbevoegde toegang tot ICTvoorzieningen.
**BIO:** De Baseline Informatiebeveiliging Overheid (BIO) is geheel gestructureerd volgens NEN-ISO/IEC 27001:2017, bijlage A en NEN-ISO/IEC 27002:2017. Het Forum Standaardisatie heeft deze normen opgenomen in de 'pas toe-of-leg uit'- lijst met verplichte standaarden voor de publieke sector, volgens het comply or explain principe. Dit betekent dat de overheid deze normen toepast tenzij er expliciet geformuleerde redenen zijn om dit niet te doen.
De BIO beschrijft de invulling van de NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017 voor de overheid. Met klem vermeldt zij dat de BIO deze normen niet vervangt.
**BRP:** Basis Registratie Personen
**CERT:** Computer Emergency Response Team (CERT) is een gespecialiseerd team van ICT-professionals, dat in staat is snel te handelen in het geval van een beveiligingsincident met computers of netwerken. Het doel is om schade te reduceren en snel herstel van de dienstverlening te bevorderen. Naast reactie op incidenten richt een CERT zich ook op preventie en preparatie.
**CSIRT:** Een collectief Computer security Incident Response Team (CSIRT) is een samenwerkingsvorm die kan ontstaan vanuit een reeds bestaande samenwerking, bijvoorbeeld een Information Sharing and Analysis Centre (ISAC).
**Common Ground: E**en gezamenlijke informatievoorziening voor het uitwisselen van gegevens
**Controleerbaarheid:** De mate waarin de werkelijkheid of representaties daarvan toetsbaar zijn, dat wil zeggen te vergelijken met andere 'werkelijkheden of representaties daarvan' zodat objectieve oordeelsvorming mogelijk wordt ICT-voorzieningen: Applicaties en technische infrastructuur, het geheel van ICT-voorzieningen.
**Deelnemende gemeenten:** Gemeente Bunnik, Gemeente De Bilt, Gemeente Houten, Gemeente Lopik, Gemeente Nieuwegein, Gemeente Stichtse Vecht, Gemeente Utrecht, Gemeente Utrechtse Heuvelrug, Gemeente Zeist
**Deelnemende waterschap:** Hoogheemraadschap De Stichtse Rijnlanden
**DigiD:** Digitale identiteit
**IBD:** InformatieBeveiligingsDienst. De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en onderdeel van de Vereniging van Nederlandse Gemeenten. De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging en privacy. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD draagt namens gemeenten bij aan de Baseline Informatiebeveiliging Overheid (BIO) en geeft regelmatig kennisproducten uit.

**Informatiebeveiliging:** Het proces van vaststellen van de vereiste betrouwbaarheid van informatieverwerking in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van maatregelen.
**Informatiesysteem:** Een samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en programmatuur en de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie. Integrale beveiliging is de beveiliging van vastgestelde te beschermen belangen door op basis van risicomanagement en een kosten/batenanalyse een samenhangend stelsel van beveiligingsmaatregelen te selecteren en te implementeren. Het besturingsmodel voor integrale beveiliging sluit aan bij de besturingsuitgangspunten binnen de BghU: het lijnmanagement is integraal verantwoordelijk en dus ook voor de beveiliging.
**Integriteit:** Het waarborgen van de juistheid, volledigheid en tijdigheid van informatie en de verwerking ervan. Als de tijdigheid van gegevens bepaald wordt door omstandigheden buiten het systeem, kan deze vanzelfsprekend niet als integriteitseis voor het systeem gesteld worden.
**IoT:** Internet of Things. Onze wereld wordt steeds digitaler. Niet alleen wij mensen, maar ook de dingen om ons heen zijn steeds meer verbonden. Machines, auto's, koelkasten en zelfs landbouwgronden, dijken en gebouwen. Zo'n beetje alle 'dingen' kunnen verbonden worden met het internet. Hiervoor wordt gebruikgemaakt van sensoren en andere speciale hardware. Zodra deze 'dingen' online zijn, kunnen ze communiceren. Met elkaar, met hun gebruikers, met organisaties en andere verbonden partijen. Dat is het internet der dingen oftewel the Internet of Things.
**ISMS:** Het Information Security Management System is een procesgerichte benadering voor informatiebeveiliging. Het is een managementsysteem waarin het risicobeheerproces centraal staat, zodat risico's adequaat worden beheerd. Het ISMS is de motor van de informatiebeveiligingsactiviteiten en wordt onderhouden middels de plan-do-check-act cyclus. Het doel van het ISMS is het continu beoordelen of beveiligingsmaatregelen passend en effectief zijn, en of deze bijgesteld moeten worden. Het helpt organisaties onder andere om risico's te beheersen, passende beveiligingsmaatregelen te treffen, lering te trekken uit incidenten en daarmee de betrouwbaarheid van de informatievoorziening en bedrijfscontinuïteit te waarborgen.
**NCSC:** Nationaal Cyber Security Centrum
**NEN ISO/IEC 27001:2017:** informatiebeveiligingsnorm ISO 27001
**NHR:** Basisregistratie Nationaal Handelsregister
**NORA:** Nederlandse Overheid Referentie Architectuur
**Onweerlegbaarheid:** Het niet kunnen ontkennen iets te hebben gedaan (bijvoorbeeld een bericht te hebben ontvangen dan wel te hebben verstuurd).
**PDCA:** Een afkorting die staat voor de belangrijkste stappen uit de cirkel: Plan (maak een plan met de resultaten die je wilt bereiken), Do (voer het plan uit), Check (vergelijk de resultaten met wat je had willen bereiken), Act (bij afwijking: neem maatregelen/stuur bij om de resultaten alsnog te bereiken)
**Phishing:** Is een vorm van internetfraude waarbij een slachtoffer valse e-mails ontvangt die de slachtoffer naar een nagebootste website proberen te lokken.
**Technische infrastructuur:** Het geheel van ICT-voorzieningen voor generiek gebruik, zoals servers, firewalls, netwerkapparatuur, besturingssystemen voor netwerken en servers, database management systemen en beheer- en beveiligingstools, inclusief bijbehorende systeembestanden.
**VCIB:** Vertrouwelijke Contactpersoon InformatieBeveiliging
**Vertrouwd:** In overeenstemming met een door een bevoegde autoriteit vastgesteld beveiligingsniveau. Bijvoorbeeld vertrouwde zones of vertrouwde netwerken.
**Vertrouwelijkheid:** Het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd.
**Vertrouwelijke informatie:** Informatie die niet algemeen bekend mag worden (bron: van Dale). In het kader van de BIO worden maatregelen beschreven die voldoen voor de behandeling van gerubriceerde informatie tot en met vertrouwelijke en persoonsvertrouwelijke informatie, zoals bedoeld de AVG.
**VNG:** Vereniging van Nederlandse Gemeenten
**WOZ:** Wet waardering Onroerende Zaken