Belastingsamenwerking
gemeenten & hoogheemraadschap Utrecht

IBP

Informatie BeveiligingsPlan 2018

INHOUD

0.1 ALGEMEEN

0.1.1 BRONVERMELDING

In dit document is het informatie beveiligingsplan (IBP) van de Belastingsamenwerking gemeenten & hoogheemraadschap Utrecht (BghU) beschreven. De eerste versie van dit plan dateert uit 2015: gebaseerd op een nadere uitwerking van het voorbeeld informatiebeveiligingsbeleid van Kwaliteitsinstituut Nederlandse Gemeenten (KING) [1] hetgeen in augustus 2013 is opgesteld [2]. Het beheer van genoemde document berust bij de Informatie BeveiligingsDienst voor gemeenten (IBD).
Verder is rekening gehouden met 'hogere' regelgeving zoals Wet Bescherming Persoonsgegevens, Wet computercriminaliteit, Baseline Informatiebeveiliging Gemeenten (BIG) en Wet Datalekken. Afbeeldingen afkomstig van https://nl.freeimages.com/

BghU IBP wordt jaarlijks bijgewerkt op basis van veranderende wetgeving, taken, risico's en bedreigingen. Tussentijds of geplande geïmplementeerde maatregelen worden in IBP verwerkt.

0.1.2 DEELNEMERS

Voor het actief uitdragen van het informatie beveiligingsplan is binnen BghU een klankbordgroep IBP geformeerd met vertegenwoordigers uit de BghU procesteams.

Deze werkgroep bestaat uit:
Erik Verheul
Gert Grobben
Henri van Wijk
Niek Hofstetter
Marius van den Akker
Rik van Deijl
Monique van der Werf
Bart Boersma
Sammy Lee
Jan Douwe de Jong

[1] KING: naamgeving inmiddels gewijzigd in VNG Realisatie.

0.1.3 VERSIE HISTORIE EN DISTRIBUTIE

Nr.	Datum	Status	Beschikbaar gesteld aan	Fase
0.1	Mei 2018	Concept	Klankbordgroep	Commentaar ronde
0.2	22 mei 2018	Concept	Directie	Ter goedkeuring
1.0	**24 mei 2018**	**Definitief**	**Directie**	**Vastgesteld**

0.1.4 BELANGRIJKSTE WIJZIGINGEN IBP

0.1.4.1 HET AFGELOPEN JAAR:

- BghU aangesloten IBD
- AVG [3] rol Functionaris Gegevensbescherming (FG) geformaliseerd.
- AVG rol Security Officer (CISO) geformaliseerd.
- Procedure melding en afhandeling DataLek intern en met leveranciers afgestemd.
- Register DataLekken ingesteld.
- E-herkenning voor ondernemers geïmplementeerd.

0.1.4.2 HET KOMENDE JAAR:

- Voortaan jaarlijkse check 'beveiligingscultuur en bewust zijn van IBP'.
- Inrichten van deelnemersportaal: voor veilig, gebruiksvriendelijk en registratie van uit te wisselen bestanden.
- Uitvoeren Privacy Impact Analyse PIA (komt voort uit AVG) handelen waar nodig.
- Implementatie eIDAS [4]: Europese burgers en ondernemers moeten in september 2018 veilig kunnen inloggen MijnBghU met eigen nationale inlogmiddel,
- Invoeren extra beveiliging handeling voor BghU medewerkers bij inloggen op kantoor: deze maatregel wordt ingevoerd omdat we 'eenmalig inloggen' voor het benaderen van meerdere applicaties in 2018 uitrollen. De handeling bestaat uit het via een token genereren van een korte tijd geldige beveiligingscode welke naast inlognaam en wachtwoord ingevoerd moet worden.

[3] AVG: Algemene Verordening Gegevensbescherming.

[4] eIDAS = EU verordening: regelt dat burgers en bedrijven welke voorkomen in database veilig moeten kunnen inloggen.

HOOFDSTUK 1. SCOPE

Doel van informatiebeveiliging

De toenemende afhankelijkheid van informatiesystemen en informatiestromen leidt tot risico's voor de continuïteit van de dienstverlening van de belastingsamenwerking gemeenten & hoogheemraadschap Utrecht (BghU). Betrouwbare, beschikbare en correcte informatie is cruciaal voor de primaire processen en bedrijfsvoering.
Na diverse incidenten rondom informatiebeveiliging bij overheidsorganisaties en de toenemende cybercrime heeft de Tweede Kamer en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) de druk opgevoerd om maatregelen te nemen die de digitale veiligheid garanderen. Het Ministerie van BZK heeft om dit te bereiken de Taskforce Bestuur Informatieveiligheid en Dienstverlening opgericht. Ook bij de BghU komt het belang voor dit onderwerp steeds meer naar voren. Eén van de zaken die naar aanleiding van eerdere beveiligingsincidenten zijn ingevoerd is elk jaar uitvoeren van een DigiD assessment door een externe onafhankelijke auditor.

Dit informatiebeveiligingsbeleid is er op gericht de beschikbaarheid, de integriteit en de vertrouwelijkheid van de (geautomatiseerde) gegevensuitwisseling binnen onze organisatie te waarborgen. Om de beheersbare en betrouwbare informatievoorziening te realiseren, is het van belang een aantal gemeenschappelijke uitgangspunten te hanteren en deze uit te dragen.

Het informatiebeveiligingsbeleid heeft als doel om de betrouwbare werking van de (geautomatiseerde) uitwisseling van informatie van en naar onze organisatie inzichtelijk te maken. Tevens worden de maatregelen aangegeven die verstoringen en inbreuken tegengaan.

1.2 DEFINITIE INFORMATIEBEVEILIGING

Informatiebeveiliging is het treffen en onderhouden van een samenhangend pakket maatregelen, gericht op het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening. Het gaat hierbij om:

Preventieve maatregelen: het voorkomen van informatiebeveiligingsproblemen;

Repressieve maatregelen: het beperken van schade als gevolg van informatiebeveiligingsproblemen;

Correctieve maatregelen: de schade die is ontstaan door informatiebeveiligingsproblemen herstellen.

Onderstaand is de definitie van beschikbaarheid, integriteit en vertrouwelijkheid gegeven.

Beschikbaarheid: waarborgen dat geautoriseerde gebruikers en klanten op de juiste momenten toegang hebben;

Integriteit: het waarborgen van de juistheid, actualiteit en de volledigheid van informatie;

Vertrouwelijkheid: het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn.

In dit document wordt met de term informatiesysteem bedoeld het geheel van mensen, middelen, processen en regels dat de informatievoorziening verzorgt.

HOOFDSTUK 2. INFORMATIEBEVEILIGINGSBELEID

Doelstelling

Borgen van betrouwbare dienstverlening en een aantoonbaar niveau van informatiebeveiliging dat voldoet aan de relevante wetgeving, algemeen wordt geaccepteerd door haar (keten-)partners en er mede voor zorgt dat de kritische bedrijfsprocessen bij een calamiteit of incident voortgezet kunnen worden.

Beleidsdocumenten voor informatiebeveiliging

Een document met informatiebeveiligingsbeleid behoort door de directie te worden goedgekeurd en aan alle medewerkers beschikbaar gesteld te worden. Het document dient tevens kenbaar te worden gemaakt aan relevante externe partijen.

2.1 BGHU SPECIFIEKE MAATREGEL

Er is beleid voor informatiebeveiliging door de directie vastgesteld, beoordeeld op basis van inzicht in risico's, kritische bedrijfsprocessen en toewijzing van verantwoordelijkheden en prioriteiten.

Beoordeling van het informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid behoort met geplande tussenpozen, of zodra zich belangrijke wijzigingen voordoen, te worden beoordeeld om te bewerkstelligen dat het geschikt, toereikend en doeltreffend blijft.

2.2 BGHU SPECIFIEKE MAATREGEL

Het informatiebeveiligingsbeleid wordt één keer per jaar, of zodra zich belangrijke wijzigingen voordoen, beoordeeld en zo nodig bijgesteld.

HOOFDSTUK 3 BEVEILIGINGSORGANISATIE

Doelstelling

Beheren van de informatiebeveiliging binnen de organisatie.

De directie behoort actief informatiebeveiliging binnen de organisatie te ondersteunen door duidelijk richting te geven, betrokkenheid te tonen en expliciet verantwoordelijkheden voor informatiebeveiliging toe te kennen en te erkennen.

3.1 ORGANISATIE VAN DE INFORMATIEBEVEILIGING

In deze paragraaf is aangegeven op welke wijze dit wordt uitgevoerd.

De CISO formuleert in overleg met de informatiemanager het IBP beleid van de organisatie. De directie van de BghU waarborgt de informatiebeveiligingsdoelstellingen en stelt beleid vast. De CISO en FG controleert uitvoering IBP beleid. CISO en FG krijgen ondersteuning van ICT-beheerders, zo nodig medewerker AO/IC [5] en een juridisch medewerker voor monitoren uitvoering van het opgestelde beleid en zorgt voor de actualiteit hiervan. Periodiek wordt in het directieoverleg informatiebeveiliging en informatiebeheer besproken. Indien noodzakelijk wordt specialistisch advies over informatiebeveiliging ingewonnen. Bijvoorbeeld door overleg met leverancier van BghU ICT-omgeving/integraal belastingsysteem of dat externe specialisten worden ingehuurd.

Het Management Team (MT) als product eigenaren van de BghU procesteams zijn mede verantwoordelijk voor uitvoering van het opgestelde beleid. Concreet betekent dit dat zij een actieve rol hebben in het vergroten van de bewustwording bij medewerkers inzake het correct omgaan met informatie. IBP aspecten worden jaarlijks besproken tijdens integrale BghU lunchbijeenkomst en in het reguliere overleg van alle procesteams. Via NarrowCasting teasers[6] en nieuwsbrief worden IBP-items meer frequent onder aandacht gebracht. Het BghU IBP wordt integraal beschikbaar gesteld op BghU intranet met leesverplichting en besproken met de Ondernemingsraad[7] (OR), ICT leveranciers Centric en gemeente Utrecht in de rol van ICT leverancier en printbedrijf DataB.

[5] AO/IC: Administratieve Organisatie / Interne Controle.

[6] Prikkelende tekst weergegeven op beeldkrant.
Voorbeeld: "Weg van je werkplek? Vergeet je schermbeveiliging niet te activeren."

[7] Op agendapunt overleg OR juni 2018.

3.2 BEVEILIGING VAN TOEGANG TOT INFORMATIE

3.2.1 MEDEWERKERS

De BghU geeft in deze paragraaf uitleg over de maatregelen die genomen zijn om toegang tot informatiesysteem te beheersen.

Inzage van persoonsgegevens binnen applicaties vanuit kantoorwerkplek is alleen mogelijk nadat een medewerker via een op naam gesteld inlogaccount met wachtwoord beveiliging inlogt. In geval een medewerker vanaf een externe locatie inlogt [8], dient er als extra toegang beveiliging een tokencode ingevoerd te worden. Op basis van een autorisatieprofiel krijgt de medewerker toegang. Relevantie mutaties die een medewerker verricht worden op datum, tijd en gebruikersnaam geregistreerd (logging), de relevante mutaties zijn besproken en afgestemd met de accountant. (Het is technisch niet mogelijk alle mutaties te loggen, de prestaties van het systeem laten dit niet toe).
Zonder de inlogprocedure[9] te doorlopen kan geen gebruik gemaakt worden van het BghU netwerk.

Een medewerker is tot geheimhouding verplicht van hetgeen hem in verband met zijn functie ter kennis is gekomen, voor zover die verplichting uit de aard der zaak volgt, aldus artikel 125a, derde lid, van de Ambtenarenwet. Voor sommige ambtenaren bestaat daarnaast ook nog een bijzondere geheimhoudingsplicht (bijvoorbeeld op grond van art. 67 Invorderingswet). Daarnaast kent de Algemene wet bestuursrecht (artikel 2:5) een algemene geheimhoudingsplicht voor een ieder voor wie niet al op grond van ambt, beroep, of wettelijk voorschrift een geheimhoudingsplicht geldt voor die gegevens waarvan zij het vertrouwelijk karakter kennen of redelijkerwijs moeten vermoeden. Inhuurkrachten dienen bij het (tijdelijk) in dienst treden een geheimhoudingsverklaring te tekenen (Bijlage III). Van elke nieuwe inhuurkracht wordt een VOG[10] (Verklaring Omtrent Gedrag)[11] gevraagd als de persoon niet via een leverancier of opdrachtnemer die een bewerkersovereenkomst heeft getekend, is ingehuurd. Van medewerkers die inmiddels langer dan 2 jaar werkzaam zijn voor de BghU is een VOG niet nodig.

3.2.2 DERDEN

In overeenkomsten met derden, waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of ICT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan ICT-voorzieningen, behoren alle relevante beveiligingseisen te zijn opgenomen.

---

[8] Wanneer in 2018 eenmalig inloggen (Single SignOn) gerealiseerd is zal ook extra tokencode voor toegang via kantoorwerkplek vereist zijn: zie ook paragraaf 0.1.4.2.

[9] Voor authenticatie en autorisatie wachtwoord/ toegangbeveiligingsbeleid.

[10] Indien geen inlog toegang tot systeem is geen VOG nodig. (Bijvoorbeeld bij adviseur).

[11] Betreft Algemeen screeningsprofiel gericht op financieel/administratief risicogebied.

Uitbesteding (beheer, ontwikkelen en aanpassen) van software is geregeld volgens formele contracten waarin o.a. intellectueel eigendom, kwaliteitsaspecten, beveiligingsaspecten, aansprakelijkheid, escrow[12] geregeld worden.

In Service Level Agreement (SLA) met externe partijen is vastgelegd hoe men om dient te gaan met wijzigingen en hoe ervoor gezorgd wordt dat de beveiliging niet wordt aangetast door de wijzigingen.

Alvorens derden werkzaamheden voor of namens de BghU verrichten, wordt door deze persoon een Verklaring Omtrent Gedrag verstrekt (VOG), een VOG is niet nodig wanneer een medewerker ingehuurd is van een inhuurbedrijf die met de BghU een bewerkersovereenkomst heeft afgesloten.

In contracten met externe partijen is vastgelegd hoe escalaties en aansprakelijkheid geregeld zijn.

Voor onderaannemers gelden dezelfde beveiligingseisen als voor de hoofdcontractant. De hoofdaannemer is verantwoordelijk voor de borging bij de onderaannemer van de gemaakte afspraken.

De producten, diensten en daarbij geldende randvoorwaarden, rapporten en registraties die door een derde partij worden geleverd, worden beoordeeld op het nakomen van de afspraken in de overeenkomst. Verbeteracties worden geïnitieerd wanneer onder het afgesproken niveau wordt gepresteerd.

3.2.3 KLANTENCONTACTEN

Contact met onze klanten vindt plaats via telefoon, fysiek (deurwaarders, taxateurs, bestandcontroleurs, afvalwatertechnoloog, balie medewerkers), via de BghU digitale balie en MijnOverheid.nl. Via de digitale balie kunnen klanten informatie raadplegen/aanvragen/muteren over aan hen opgelegde aanslagen, brongegevens en betaalgegevens. Alle voor de klant relevante informatie wordt via beveiligde koppelvlakken verkregen uit de database van ons belastingsysteem.

Door de digitale balie kunnen en mogen niet rechtstreeks mutaties op de gegevens van het belastingsysteem worden aangebracht. Mutaties worden via een tussentabel aangeboden en na verificatie verwerkt.

Voor toegang tot de gegevens wordt gebruikgemaakt van een database-user met beperkte rechten.

[12] Escrow is een overeenkomst tussen de maker van software, zijn klanten en een escrow-agent. De overeenkomst garandeert dat de klant in bepaalde gevallen kan beschikken over de laatste broncode van het softwarepakket waarvoor de overeenkomst gesloten is. (Voorbeeld: faillissement leverancier).

3.3 UITBESTEDING

Voor kantoorautomatisering, primaire applicaties en digitale diensten wordt gebruik gemaakt van externe leveranciers. Het door de BghU vastgestelde beveiligingsniveau wordt door deze leveranciers[13] ondersteunt. Met alle externe leveranciers is een bewerkersovereenkomst afgesloten.

HOOFDSTUK 4. CLASSIFICATIE EN BEHEER VAN BEDRIJFSMIDDELEN

4.1 VERANTWOORDING VAN BEDRIJFSMIDDELEN

In deze paragraaf wordt aangegeven op welke manier de BghU haar bedrijfsmiddelen beveiligt tegen verstoringen. Alle belangrijke informatiebedrijfsmiddelen zijn bij de BghU beveiligd.

Er wordt een actuele registratie van bedrijfsmiddelen (CMDB) bijgehouden die voor de organisatie een belang vertegenwoordigen, zoals gegevens(verzamelingen), software, hardware, diensten.

4.2 CLASSIFICATIE VAN INFORMATIE

In deze paragraaf wordt aangegeven op welke wijze informatie binnen de BghU is gecategoriseerd.

Binnen de BghU wordt gewerkt met persoonsgegevens die aangemerkt kunnen worden als bijzondere persoonsgegevens zoals beschreven in artikel 16 Wet Bescherming Persoonsgegevens. Van de gegevens die door de BghU, via DigiD beveiligde website, beschikbaar worden gesteld aan de burger, zijn de gegevens in bijlage II als privacy gevoelig aangewezen.

4.2.1 BACK-UP

Om te voorkomen dat medewerkers bij een eventuele crash van het netwerk voor langere tijd niet kunnen beschikken over de voor hen relevante informatie, wordt dagelijks een back-up gemaakt van alle servers/informatiesystemen. Concreet betekent dit, dat alle gegevens die zich op de servers bevinden (data, rapporten, beschikkingen etc.) elke dag worden veiliggesteld. Het feitelijk uitvoeren van de back-up wordt uitgevoerd door de beherende organisatie. Afspraken over veiligstellen van de informatie zijn vastgelegd in een overeenkomst.

[13] Overzicht leveranciers: zie Bijlage I.

HOOFDSTUK 5 BEVEILIGINGSEISEN TEN AANZIEN VAN PERSONEEL

5.1 BEVEILIGINGSEISEN BIJ AANNAME VAN PERSONEEL

Door middel van deze paragraaf wordt in kaart gebracht op welke manier de BghU aandacht schenkt aan informatiebeveiliging ten aanzien van personeel.

5.1.1 MEDEWERKERS MET EEN VASTE OF TIJDELIJKE AANSTELLING

Personeel dat in dienst is bij de BghU valt direct onder de Arbeidsvoorwaardenregeling gemeente Utrecht (ARU). Daarnaast is de basisgedragscode BghU van toepassing. Hierin is geregeld dat zij bij in diensttreding een integriteitsverklaring ondertekenen. Medewerkers krijgen na hun benoeming een inwerktraject. Elke medewerker heeft de verplichting alle zaken, waarvan hij weet of vermoedt dat ze een vertrouwelijk karakter hebben, geheim te houden.

Ook dienen medewerkers ingevolge de Wet op de Identificatieplicht vooraf aan het in diensttreding hun legitimatiebewijs te laten zien. Hier wordt een kopie van gemaakt t.b.v. het personeelsdossier. Tevens dienen medewerkers voor indiensttreding een Verklaring Omtrent Gedrag (VOG) te overleggen.

5.1.2 EXTERNE MEDEWERKERS

Medewerkers die werkzaamheden verrichten bij de BghU en niet in een ambtelijk dienstverband zijn benoemd, zijn gedetacheerd via een uitzendbureau of op andere wijze ingehuurd. In geval het inhuurbedrijf geen bewerkersovereenkomst met BghU heeft, dient inhuurkracht een Verklaring Omtrent Gedrag (VOG) te verstrekken voor aanvang van de BghU werkzaamheden. Dit geldt dus altijd voor ZZP'ers.

5.1.3 NIEUWE MEDEWERKERS

Voor aanvang van de BghU werkzaamheden krijgen alle nieuw in dienst tredende (vast/tijdelijk/inhuur) medewerkers het Informatie Beveiligingsplan ter beschikking.
De manager van deze nieuwe functionaris is verantwoordelijk hiervoor en regelt dit.
Van de nieuwe functionaris wordt verwacht voor aanvang van de betrekking het IBP door te hebben gelezen en zich te conformeren door verklaring te ondertekenen[14].

[14] Bijlage III.

5.1.4 MUTATIE DIENSTVERBAND MEDEWERKERS

Bij het beëindigen van het dienstverband van een medewerker wordt door HRM een melding gedaan bij ICT-beheer. Om misbruik van de accountgegevens te voorkomen, zorgt ICT-beheer voor het onmiddellijk blokkeren van het account. Daarnaast zorgt ICT-beheer ervoor, via een wijzigingsverzoek naar leverancier, dat het account wordt verwijderd. De leverancier geeft in de kwartaal rapportage een overzicht van opgevoerde en afgevoerde accounts, alsmede gewijzigde autorisatieprofielen van bestaande medewerkers.

5.2 TRAINING VOOR GEBRUIKERS

Vanaf haar oprichting 1 januari 2014 instrueert BghU haar medewerkers omtrent correcte omgang met ICT-voorzieningen en stelt gebruikershandleidingen en werkinstructies ter beschikking. In augustus 2016 is de BghU-academie gelanceerd. Binnen de BghU academie kunnen medewerkers kennissessies volgen, vak- en systeemkennis vergroten en werken aan persoonlijk loopbaan ontwikkeltraject. Met ingang van het 2e kwartaal 2018 zal ook de kennissessie 'doel en noodzaak IBP' aangeboden worden.

5.3 REAGEREN OP INCIDENTEN EN STORINGEN

In deze paragraaf is aangegeven op welke wijze de BghU incidenten, die de beveiliging aantasten, verwerkt en registreert.

Wanneer zich binnen de BghU een ICT technische melding voordoet, wordt dit kenbaar gemaakt aan ICT-beheer en geregistreerd. De medewerkers ICT-beheer: classificeren, prioriteren, lossen issue op of zetten dit uit bij leverancier, bewaken en rapporteren inzake voortgang en communiceren terug binnen BghU organisatie.
ICT-infrastructuur is in toenemende mate van cruciaal belang voor het uitvoeren van de BghU bedrijfsprocessen. Voor het vastleggen en bewaken van incidenten wordt gebruik gemaakt van de ondersteunende applicatie Topdesk. Iedere BghU medewerker heeft toegang tot TopDesk. Beveiligingsincidenten worden gemeld aan informatiemanager, directie en vastgelegd binnen TopDesk.

5.3.1 OPTREDEN BIJ CALAMITEITEN

Als er (mogelijk) sprake is van een calamiteit, dan treedt het calamiteitenplan BghU – Centric in werking. Dit plan is beschikbaar op BghU netwerk, bij BghU ICT-beheer (brandkast) en bij Centric.

5.3.2 LERING TREKKEN UIT INCIDENTEN

Met behulp van TopDesk, zoals eerder is aangegeven, is BghU beter in staat lering te trekken uit voorgaande incidenten en wijzigingen. Vanuit de afhandeling van incidenten en wijzigingen, wordt het kennissysteem in TopDesk verder uitgebouwd. In toenemende mate kunnen gebruikers via FAQ's[15] of door intypen van zoekvragen informatie raadplegen.

[15] FAQ = veel gestelde vragen

HOOFDSTUK 6. FYSIEKE BEVEILIGING EN BEVEILIGING VAN DE OMGEVING

6.1 BEVEILIGDE RUIMTEN

Deze paragraaf geeft inzicht in de wijze waarop BghU de ICT voorzieningen heeft beschermd tegen ongeoorloofde toegang, schade en storingen.

BghU is afhankelijk van ICT-voorzieningen voor het verrichten van de primaire processen. Uitval van deze voorzieningen heeft als risico dat er geen aanslagen worden opgelegd en voldaan.

Het beheer van ICT-voorzieningen is door BghU uitbesteed aan een derde partij. BghU heeft dus geen serverruimte in eigen beheer. Wel zijn er binnen het gebouw van BghU actieve netwerkcomponenten aanwezig. Toegang tot deze apparatuur is slechts toegestaan voor de externe beheerder. Door middel van het fysiek afsluiten van deze ruimten is ongeoorloofde toegang geborgd.

Bij storingen aan de ICT-voorzieningen worden de leveranciers ingeschakeld om de geconstateerde problemen op te lossen. Dit overeenkomstig de contracten met de leveranciers en het calamiteitenplan BghU – Centric

6.2 FYSIEKE BEVEILIGING VAN DE OMGEVING EN HET GEBOUW

BghU heeft twee balies op de tweede etage van het stadskantoor gemeente Utrecht die toegankelijk zijn voor het publiek, alsmede een afgesloten kantoor annex overlegruimte. De niet voor publiek toegankelijk ruimten kunnen alleen geopend worden door geautoriseerde medewerkers met een geldige toegangspas..

6.2.1 DE OMGEVING EN HET GEBOUW

Het gebouw is voorzien van inbraakbeveiliging. Hiervoor is een contract afgesloten door de verhuurder, de gemeente Utrecht. Daarnaast wordt de omgeving beveiligd door middel van een camerasysteem. Ook is er op elke publiek toegankelijke verdieping een beveiliger aanwezig en een gastvrouw/gastheer om publiek wegwijs te maken.

6.2.2 INGANG

De centrale publiek ingang wordt beveiligd met behulp van videobewaking. De personeelsingang, parkeergarage en fietsenstalling is tevens voorzien van een toegangspas systeem. Alle medewerkers van de BghU zijn in bezit van een elektronische pas om de toegangsdeuren of -poortjes te openen.

6.2.3 BALIE

Bij de inrichting van de balie van de BghU is rekening gehouden met fysieke beveiliging aspecten. Zonder toegangspas kan men alleen achter de balie komen door over de relatief hoge balie heen te klimmen. BghU balies beschikken over een calamiteitenknop en liften mee met beveiligingsprocedure van de gemeente Utrecht. In geval van calamiteiten wordt door de bewaking ingegrepen. Contant geld wordt door BghU medewerker direct na ontvangst afgestort in een niet tijdens kantooruren te openen contant geld afstort voorziening.

6.2.4 DE WERKRUIMTEN

Voor toegang tot de BghU werkruimten op de 2e, 15e en 16e etage van de zuidtoren stadskantoor gemeente Utrecht wordt een pasjessysteem voor openen toegangsdeuren of -poortjes gehanteerd.

Bezoekers of derden kunnen alleen toegang krijgen tot de 15e en 16e etages nadat ze door BghU medewerker op de 6e etage opgehaald zijn. Deze Bezoekers of derden worden onder de verantwoordelijkheid van deze BghU medewerker toegelaten. De BghU medewerker is gedurende het bezoek verantwoordelijk voor deze bezoeker of derden.

Onderhoudsmedewerkers van leveranciers, installatiebedrijven etc. die geacht worden werkzaamheden te verrichten, dienen zich te kunnen legitimeren als zijnde medewerker van het betreffende bedrijf.

6.3 BEVEILIGING VAN APPARATUUR

6.3.1 HET PLAATSEN EN BEVEILIGEN VAN APPARATUUR

Actieve componenten ten behoeve van de ICT infrastructuur zijn in afgesloten ruimte(n) geplaatst waartoe alleen geautoriseerde medewerkers toegang hebben. Het is in deze speciale ruimte(n) niet toegestaan om andere apparaten te plaatsen die niet actief deelnemen aan het netwerk (koffieapparaat, printer, schoonmaakspullen etc.).

6.3.2 STROOMVOORZIENING

De externe beheerder van de BghU infrastructuur heeft maatregelen getroffen om bij uitval van de stroomvoorziening apparatuur operationeel te houden: garandeert een beschikbaarheid groter dan 99%.

6.3.3 BEVEILIGING VAN KABELS

Alle bekabeling, van stroom- tot communicatiebekabeling, is beveiligd tegen interceptie of beschadiging. Hiervoor is de norm NEN 1010 in acht genomen.

6.3.4 ONDERHOUD VAN APPARATUUR

Het onderhoud van apparatuur wordt verzorgd door de ICT- leverancier gemeente Utrecht in overleg met de informatiemanager van BghU.

6.3.5 BEVEILIGING VAN APPARATUUR BUITEN DE LOCATIE

Voor apparaten, die eigendom zijn van de BghU en bestemd zijn voor werken buiten het kantoorpand, zijn beveiligingsmaatregelen getroffen. Op mobiele apparatuur wordt via internet uitsluitend over een beveiligde verbinding ingelogd op het netwerkdomein van BghU: het is niet mogelijk bestanden vanuit BghU te verplaatsen naar geheugenopslag van het apparaat zelf. De inlogprocedure is beschreven in paragraaf 3.2.

Laptops, tablets en smartphones, zijn –naast toegangsbeveiliging en encryptie- voorzien van software waarmee, in geval van verlies of diefstal, de inhoud op afstand gewist zal worden en het desbetreffende apparaat geblokkeerd voor toegang tot het BghU-netwerk. Ook met een laptop is het BghU netwerk via een browser (uitsluiten via een beveiligde verbinding) te benaderen. Inloggen werkt op dezelfde wijze als via werkstation in het BghU kantoorgebouw, voor toegang via een laptop is een extra token beveiligingscode nodig om succesvolle inlog te voltooien.

6.3.6 VEILIG AFVOEREN EN HERGEBRUIKEN VAN APPARATUUR

Bij uitfasering van apparatuur wordt door de ICT-beheerders in samenwerking met de ICT-leverancier gevoelige informatie verwijderd: door geheugenopslag te vernietigen dan wel geheugenopslag minimaal 7 maal willekeurig met 0 en 1 bytes te overschrijven, zodat

opnieuw leesbaar maken niet mogelijk is. Deze aanscherping komt voort uit invoering wet op Datalekken 1 januari 2016.

6.4 ALGEMENE BEVEILIGINGSMAATREGELEN

Ongeautoriseerde toegang wordt voorkomen door een standaard schermbeveiliging met wachtwoord die alle beeldschermen na een korte periode van inactiviteit blokkeert. Bij het verlaten van de werkplek, wordt van elke BghU medewerker verwacht zijn of haar werkstation te vergrendelen.

6.4.1 CLEAN DESK

De BghU hanteert een clean desk policy. Dat wil zeggen dat het de medewerkers niet is toegestaan om privacy gevoelige informatie onbeheerd op het bureau achter te laten en om na werktijd persoonlijke eigendommen achter te laten op of bij de werkplek. Elke medewerker heeft toegang tot een afsluitbare ruimte waar hij/zij zaken kan opbergen. Ten einde te voorkomen dat papierendocumenten met persoonsgegevens bij BghU kantoorprinters blijven liggen, kan uitsluitend met 'follow me' printen, dat wil zeggen: papier rolt pas uit printer wanneer medewerker een persoonlijke code invoert op printer.

6.4.2 BEWUSTWORDINGSCAMPAGNE

Om IBP onder de aandacht van de medewerkers te brengen en te houden, worden er verschillende activiteiten georganiseerd. Bij het in diensttreden is er een verklaring vereist dat er kennis is genomen van IBP. Daarnaast wordt er jaarlijks en tijdens integrale BghU lunchbijeenkomst en in sessies van alle procesteams nieuwe IBP aspecten besproken en de meest belangrijke IBP-aspecten herhaald. Via NarrowCasting teasers[16] en nieuwsbrief worden IBP-items meer frequent onder aandacht gebracht en is het IBP integraal beschikbaar op BghU intranet. Door deze middelen beoogt BghU een cultuur te versterken dat medewerkers elkaar aanspreken wanneer de vertrouwelijkheid van gevoelige gegevens onnodig gevaar lopen.

[16] Prikkelende tekst weergegeven op beeldkrant.
Voorbeeld: "Weg van je werkplek? Vergeet je schermbeveiliging niet te activeren."

HOOFDSTUK 7. BEHEER VAN COMMUNICATIE- EN BEDIENINGSPROCESSEN

7.1 BEDIENINGSPROCEDURES EN VERANTWOORDELIJKHEDEN

BghU garandeert een correcte en veilige bediening van ICT- voorzieningen. Alle werkprocessen die gebruikt worden in het primaire proces zijn gedocumenteerd. Wijzigingen in deze processen leiden tot gewijzigde instructies.

De implementatie van eventuele aanvullende software-functionaliteiten wordt geregeld door de ICT-beheerders. In overleg met de betreffende procesteams van de BghU wordt, nadat de wijziging in de software is getest in een separate test- of ontwikkelomgeving, een datum geprikt om tot feitelijke installering in de productieomgeving over te gaan.

Wanneer op ICT-gebied veranderingen plaatsvinden, worden de medewerkers van de BghU daarover vooraf in kennis gesteld door de ICT-beheerders.
Alleen de ICT-beheerders –na goedkeuring van informatiemanager of directie- zijn bevoegd om wijzigingen in de ICT- infrastructuur aan te brengen of aan te laten brengen. Op deze manier wordt voorkomen dat op verschillende plaatsen binnen de organisatie wijzigingen worden aangevraagd dan wel doorgevoerd en wordt op deze wijze een goed wijzigingsbeheer geborgd.

Bij calamiteiten op ICT-gebied wordt gebruik gemaakt van een door BghU en de externe beheerders vastgestelde procedure[17]. Deze procedure geeft aan hoe problemen worden afgehandeld.

Iedere medewerker van de BghU heeft toegang tot ICT- voorzieningen die noodzakelijk zijn voor de uitoefening van zijn/haar werkzaamheden. Er is sprake van functiescheiding op een aantal kritieke werkzaamheden, bijvoorbeeld fiatteren, financiële gegevens, OR en HRM. Hiervoor zijn functionarissen specifiek geautoriseerd. Op deze manier wordt misbruik van voorzieningen tegengegaan. In de eerste twee weken van elk kwartaal genereert ICT-beheer autorisatieoverzichten en stelt deze overzichten veilig op een centrale plek BghU netwerk[18]. De HRM-functionaris en Business Controller[19] beoordelen in week 3 en 4 van dezelfde maand het autorisatie overzicht[20]. Het terugkoppelen van bevindingen is de verantwoordelijkheid van de Business Controller. Deze koppelt zo nodig onregelmatigheden terug aan de directie. Indien er sprake is van demotie, zal mogelijk autorisatieniveau van medewerker worden beperkt, in dat geval wordt dit aangegeven door HRM-functionaris, MT-lid of directie.
Het wijzigen van de autorisaties gebeurt door ICT-beheer.

---

[17] Zie ook Hoofstuk 5.1.3 .

[18] Alhier locatie op netwerk vermelden.

[19] Of aangewezen vervanger(s).

[20] Beoordeling: in- uit dienst en juiste autorisatie profiel.

7.2 Systeemplanning en acceptatie

Het integraal belastingpakket van de BghU wordt in service gedraaid bij de software leverancier Centric. Door de leverancier wordt continue in de gaten gehouden of de capaciteit van de verschillende BghU systemen voldoende is en rapporteert hier maandelijks over. Nieuwe releases en updates worden eerst in de test- of ontwikkelomgeving getest alvorens deze wordt geïmplementeerd in de productie-omgeving. Op deze wijze wordt het risico van verstoringen beperkt. Bij de feitelijke implementatie van wijzigingen wordt overleg gevoerd. BghU accepteert of keurt af.

7.3 Bescherming tegen kwaadaardige software

Deze paragraaf geeft de maatregelen weer die de BghU heeft genomen om het binnendringen van kwaadaardige software te voorkomen en te ontdekken.

De BghU gebruikt voor haar netwerk een firewall om kwaadaardige aanvallen van buitenaf te voorkomen. Het beheer van deze firewall ligt bij hostingpartij en is ook als zodanig opgenomen in een dienstverleningsovereenkomst.

Naast het gebruik van een firewall, gebruikt de BghU antivirus software. Deze antivirus software is zowel op de servers geplaatst als op alle werkplekken. De hosting leveranciers garanderen dat gebruikt gemaakt wordt van de laatste geactualiseerde versie. Dit is opgenomen in de contracten met leveranciers. Daarnaast is er een robuust back-up / recovery-strategie. De data wordt bewaard in een veilige en aparte locatie. De back-up wordt dagelijks gemaakt. De herstelprocedure wordt door de leverancier regelmatig getest.

7.4 Huisregels

Met de hosting leverancier zijn afspraken gemaakt over frequentie en bewaartermijnen van de back-up. Deze afspraken liggen vast in en Service Level Agreement (SLA). Deze is beschikbaar en op te vragen bij ICT-beheer.

7.5 NETWERKBEHEER

De BghU maakt naast bekabelde netwerken ook gebruik van draadloze datacommunicatie. Uitwisseling van persoonsgegevens vindt plaats op basis van versleuteling. Medewerkers zijn actief benaderd om geen bestanden met persoonsgegevens van derden via E-mail te verzenden. Het overheid en dus ook BghU-beleid voor burgers is erop gericht digitale berichten in toenemende mate digitaal aan te bieden via MijnOverheid berichtenbox. Bestanden met persoonsgegevens mogen niet gemaild worden, tenzij bestand voorzien is van encryptie[21]. (Bij twijfel: neem contact op met ICT-beheer).

7.6 BEHANDELING EN BEVEILIGING VAN MEDIA

De media met geclassificeerde gegevens wordt op een veilige manier bewaard, afgevoerd of vernietigd. Mobiele hardware met databestanden, zoals USB, flashdrive, harddrive, Cd's en Dvd's etc. worden na gebruik uitsluitend opgeborgen in een afgesloten ruimte. Bij hergebruik of vernietiging worden deze gegevensdragers ingeleverd bij ICT-beheer.

[21] Minimaal norm AES-256

HOOFDSTUK 8. TOEGANGSBEVEILIGING

8.1 BELEID TEN AANZIEN VAN TOEGANGSBEVEILIGING

Alle medewerkers binnen BghU werkzaam aan primaire processen hebben toegang tot het integraal belasting informatiesysteem. In het kader van de informatiebeveiliging en -voorziening ontvangt iedere medewerker autorisaties voor de voor hem/haar belangrijke applicatie onderdelen. Door de integrale werkwijze van uitvoeringsorganisatie BghU hebben in praktijk bijna alle BghU medewerkers toegang.

8.2 MANAGEMENT VAN TOEGANGSRECHTEN/AUTORISATIEBEHEER

In deze paragraaf worden de procedures met betrekking tot autorisatiebeheer binnen de BghU uitgelegd.

8.2.1 REGISTRATIE VAN GEBRUIKERS

Nieuwe medewerkers -aangemeld door HRM, manager of directie- ontvangen van de ICT-beheerder(s) een inlognaam en gebruikersprofiel. De ICT-beheerder maakt gebruikersprofielen aan en bepaalt -in overleg met manager of op basis van indeling procesteams- welke autorisatieprofiel een betreffende medewerker toegekend krijgt.

Voor personeel ingehuurd van derden, welke werkzaamheden verrichten voor de BghU, wordt uitsluitend een named-user account aangemaakt. De geldigheid van dit account wordt gelijkgesteld aan de contractduur. Dit om te voorkomen dat derden toegang hebben tot onze systemen na afloop van het contract.

8.2.2 SPECIALE BEVOEGDHEDEN

Er zijn bij de BghU slechts een beperkt aantal medewerkers met speciale bevoegdheden aanwezig. Met speciale bevoegdheden wordt bedoeld dat het mogelijk is dat deze medewerkers de standaard beveiliging in systemen of toepassingen te omzeilen.

De ICT-beheerders hebben de bevoegdheid om het beveiligingssysteem van de applicatie(s) te omzeilen. Dit mag alleen voor het produceren van niet standaard rapportages en/of verhelpen van productie verstorende problemen.

8.2.3 BEHEER GEBRUIKERSWACHTWOORDEN

Om te voorkomen dat medewerkers gedurende lange tijd hetzelfde wachtwoord gebruiken, verloopt na 3 maanden het netwerkwachtwoord en krijgen ze het verzoek eigen wachtwoord te wijzigen. Dit om risico op misbruik van de wachtwoorden te beperken.

8.2.4 VERIFICATIE VAN DE TOEGANGSRECHTEN

De BghU krijgt van haar Kantoorautomatisering beheerder Centric elk kwartaal een lijst met actieve en geblokkeerde gebruikers. De HRM-functionaris en Business Controller[22] beoordelen in week 3 en 4 van het nieuwe kwartaal het autorisatie overzicht[23]. Het terugkoppelen van bevindingen is de verantwoordelijkheid van de Business Controller. Deze koppelt zo nodig onregelmatigheden terug aan de directie. Indien er sprake is van demotie, zal mogelijk autorisatieniveau van medewerker worden beperkt, in dat geval wordt dit aangegeven door HRM-functionaris, MT-lid of directie.

8.3 VERANTWOORDELIJKHEDEN VAN GEBRUIKERS

De richtlijnen die gelden binnen de BghU met betrekking tot gebruik van wachtwoorden en apparatuur staan verwoord in deze paragraaf.

Effectieve beveiliging vereist de medewerking van de gebruikers. Zij dienen daarom te worden gewezen op hun verantwoordelijkheid voor het handhaven van effectieve toegangsbeveiliging, met name met betrekking tot het gebruik van wachtwoorden en de beveiliging van gebruikersapparatuur.

8.3.1 GEBRUIK VAN WACHTWOORDEN

Medewerkers van de BghU zijn verantwoordelijk voor het voorkomen van ongeautoriseerde toegang. Dit betekent dat zij op een verantwoorde wijze om moeten gaan met wachtwoorden en registratie daarvan. Naar alle medewerkers is gecommuniceerd dat wachtwoorden strikt persoonlijk zijn en niet uitgewisseld mogen worden tussen collega's.

Na eerste aanmelding dient de gebruiker het wachtwoord te wijzigen in een door hem te onthouden combinatie. Periodiek (elke 3 maanden) verschijnt de melding dat het netwerkwachtwoord verlopen is en een nieuw wachtwoord moet worden ingevoerd.

Een wachtwoord dient minimaal acht tekens lang te zijn, minimaal één cijfer te bevatten en mag maximaal 3 maanden gebruikt worden.

---

[22] Of aangewezen vervanger(s).

[23] Beoordeling: in- uit dienst en juiste autorisatie profiel.

8.3.2 ONBEHEERDE GEBRUIKERSAPPARATUUR

Voorkomen dient te worden dat tijdelijk onbeheerde gebruikersapparatuur ongeoorloofd gebruikt wordt om toegang te krijgen tot (persoons)gegevens.

Geen enkele werkstation is toegankelijk voor klanten of derden. Enkel de medewerkers van de BghU zijn bevoegd tot gebruik hiervan. In de publiekstoegankelijke ruimten zijn de computers dusdanig opgesteld en afgeschermd dat ongeoorloofd gebruik door klanten nagenoeg niet mogelijk is.

Bij het opstarten van elk werkstation is de medewerker verplicht een inlognaam en wachtwoord in te geven alvorens deze van het netwerk gebruik kan maken. Om vervolgens de primaire applicaties te starten, moet ook per applicatie een inlognaam en wachtwoord ingevoerd worden.

Bij de computers op de balies is enig risico aanwezig op ongeoorloofd gebruik, bijvoorbeeld bij afwezigheid van de medewerker. Daarom dienen medewerkers bij het verlaten van de balie uit te loggen of het systeem te vergrendelen voordat de werkplek verlaten wordt.

8.4 VERANTWOORDELIJKHEDEN VAN NETWERKEN

Het beheer van het netwerk is door de BghU uitbesteedt aan Centric en de gemeente Utrecht. Zij zijn primair verantwoordelijk voor het beheer van het netwerk.
Toegang tot openbaar internet is voor iedere medewerker en bezoeker mogelijk.

8.4.1 GEBRUIK VAN INTERNETFACILITEITEN

Het gebruik van E-mail en internet is toegestaan onder voorwaarden die zijn vastgelegd in de Uitvoeringsregeling gedragscode elektronisch verkeer (Bijlage IV). Het BghU netwerk wordt beschermt tegen bedreigingen van buiten door middel van een firewall.

8.4.2 BELEID TEN AANZIEN VAN NETWERKDIENSTEN

Iedere medewerker van de BghU kan na het inloggen op het netwerk alle beschikbare applicaties zien: medewerker kan alleen applicaties benaderen waarvoor hij/zij geautoriseerd is.

8.4.3 VERPLICHTE ROUTE

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

Binnen de BghU wordt gebruik gemaakt van een eigen netwerk (LAN) dat middels externe netwerken (WAN) is verbonden met de leverancier van de hosting. Ten behoeve van specifieke taken is het LAN-verbonden met het internet. Ook deze verbinding is voorzien van een firewall. Er is geen backdoor in de vorm van een telefoonverbinding. Het datanetwerk is getoetst aan vastgestelde normen.

8.5 Toegangsbeveiliging voor besturingssystemen

8.5.1 Netwerktoegang

Alle op het netwerk aangesloten werkstations worden bij aanmelding geïdentificeerd door de server. Na het invoeren van een persoonsgebonden gebruikersnaam en wachtwoord kan een medewerker gebruik maken van het werkstation. Bij meer dan drie foutieve aanmeldpogingen wordt het account van de medewerker geblokkeerd. Via de ICT-beheerders kan dit weer worden vrijgegeven.

De kwaliteit van wachtwoorden wordt bewaakt door het standaard wachtwoorddirectiesysteem, waardoor wachtwoorden beperkt geldig zijn en lastig te achterhalen zijn. Een wachtwoord bestaat uit minimaal 8 tekens waarvan minimaal één een cijfer en één een hoofdletter is.

8.5.2.SYSTEEMHULPMIDDELEN

De systeemhulpmiddelen beschikken over een inlogprocedure, waarbij ook gekeken wordt naar autorisaties.

8.5.3 GEBRUIK VAN WERKSTATIONS

Alle medewerkers kunnen op werkdagen tijdens de openingstijden van het kantoorgebouw aanmelden op een werkstation. Ook tijdelijke medewerkers en parttime medewerkers kunnen binnen dezelfde gestelde tijden op de dagen dat ze daadwerkelijk aanwezig zijn, gebruikmaken van een werkstation. Voor telewerken zijn geen specifieke tijden aangewezen. In het kader van het nieuwe werken kunnen medewerkers plaats en tijd onafhankelijk werken. Het inloggen op het netwerk en het gebruik van de informatiesystemen hoort daar bij.

De werkstations zijn op USB-poort niveau beveiligd, zodat er niet ongeautoriseerd data kan worden gekopieerd op losse media dragers. Er zijn een beperkt aantal medewerkers die hiervan zijn uitgezonderd, omdat specifieke werkzaamheden dit noodzakelijk maken. Deze personen zijn vastgelegd [24] en de reden is bekend. Hiervan is een overzicht op te vragen bij ICT-beheer.

[24] Alhier aangeven waar dit staat.

HOOFDSTUK 9. ONTWIKKELING EN ONDERHOUD VAN SYSTEMEN

9.1 BEVEILIGINGSEISEN VOOR SYSTEMEN

Iedere medewerker van de BghU kan op elke werkplek inloggen. Op elke werkplek die is gekoppeld aan het LAN, is de inlogprocedure gelijk. Voor externe werkplekken (telewerken etc.) is een afwijkende inlogprocedure van toepassing. Het beheer en onderhoud van het netwerk wordt verzorgd door hostingleveranciers Centric en de gemeente Utrecht.

9.2 BEVEILIGING VAN TOEPASSINGSSYSTEMEN

BghU maakt gebruik van zogenaamde thin clients . De thin clients zijn via Citrix voorzien van een virtuele desktop computers. Hierdoor is het voor medewerkers niet mogelijk zelf software te installeren. Nieuwe of vernieuwde software wordt aan de hostingleverancier Centric aangeboden met het verzoek deze te installeren en vervolgens beschikbaar te stellen.

9.3 CRYPTOGRAFISCHE BEVEILIGING

Daar waar BghU gegevens uitwisselt met derden, wordt dit via beveiligde verbindingen/versleutelde bestanden gedaan. Bestanden met privacy gevoelige gegevens worden alleen uitgewisseld met een specifiek doel en alleen als deze gegevens zijn gecomprimeerd met versleuteling en voorzien van wachtwoord. BghU heeft software pakket CitrixFileShare van leverancier Citrix geïmplementeerd voor het veilig encrypt uitwisselen van deze gegevens . Alle typen bestanden worden virtueel voor de gebruiker via een verkenner achtige structuur ontsloten; Inrichting autorisatie profiel is geregeld op basis van Need to Know. Incidenteel kan gekozen worden voor bestand uitwisseltool zoals bijvoorbeeld WeTransfer: gebruik hiervan is alleen toegestaan wanneer toegang tot bestand is beschermt via van wachtwoordbeveiliging en encryptie. Afwijkende bestandsuitwisselingen zijn niet toegestaan, voordat deze zijn beoordeeld en goedgekeurd door ICT-beheer.

9.4 BEVEILIGING BIJ ONTWIKKEL EN ONDERSTEUNINGSPROCESSEN

Wijzigingen in applicaties worden aangebracht via in paragraaf 7.2 vastgestelde wijzigingsprocedure.

HOOFDSTUK 10 : DIGITALE DIENSTEN

Burgers kunnen digitaal zaken doen met BghU. Hiervoor biedt BghU een digitale service balie: MijnBghU. Om gebruik te kunnen maken van de digitale diensten dient de klant in te loggen op de digitale balie met behulp van DigiD voor personen en eHerkenning voor ondernemers.. De eisen die DigiD en eHerkenning stelt aan beveiliging worden volledig door de BghU ondersteunt.

10.1 JAARLIJKSE BEVEILIGINGSASSESSMENT

BghU voert jaarlijks de wettelijk verplichte DigiD audit en beveiligingsassessment uit voor de MijnBghU DigiD aansluiting, Jaarlijks ook audit voor eHerkenning.

10.2 PENETRATIE TESTEN

Jaarlijks laat de BghU zogenaamde penetratie testen uitvoeren op de software en serversystemen die gebruikt worden voor het aanbieden van de digitale diensten. Bevindingen en aanbevelingen uit deze penetratietest worden beoordeeld en verwerkt in het beveiligingsbeleid.

HOOFDSTUK 11. CONTINUÏTEIT

11.1 CALAMITEITEN.

BghU heeft met hostingspartners Centric en gemeente Utrecht procedure afspraken gemaakt, wat te doen bij calamiteiten op het gebied van informatievoorziening.
Jaarlijks word samen met de hostingspartners het calamiteitenplan getest en bijgewerkt..

HOOFDSTUK 12. NALEVING

12.1 NALEVING VAN WETTELIJKE VOORSCHRIFTEN

In deze paragraaf wordt de link gelegd tussen informatiebeveiliging en wetgeving.

De BghU heeft op verschillende onderdelen te maken met wetgeving, Zaken die te maken hebben met de Algemene verordening gegevensbescherming (AVG) zijn beschikbaar in het digitale archief. Originele stukken worden vernietigd door een gecertificeerd bedrijf.

12.1.1 ALGEMENE VERORDENING GEGEVENSBESCHERMING (AVG)

Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat er vanaf die datum dezelfde privacy wetgeving geldt in de hele Europese Unie (EU). De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer. In voorbereiding op de AVG is een privacy-tool aangeschaft voor de correcte registratie van Verwerkingen, inzage door burgers en meldingen van datalekken.

12.1.2 WET OP DE DATALEK

In naleving van de Wet Meldplicht Datalekken is de BghU verplicht is om een inbreuk op de beveiliging te melden, wanneer het lekken een ernstig nadelig gevolg kan hebben op de bescherming van verwerkte persoonsgegevens. De melding moet aan de Autoriteit Persoonsgegevens worden gedaan. Om deze verplichting te borgen heeft de BghU een procedure vastgesteld. Deze procedure beschrijft de verschillende stappen die binnen BghU genomen worden bij een datalek.
Bijgevoegd als bijlage V.

12.2 Beoordeling van de naleving van het beveiligingsbeleid

Binnen de BghU is een protocol van kracht waarin medewerkers op de hoogte gesteld worden van de richtlijnen hoe om te gaan met internetgebruik.
Bijgevoegd als bijlage IV: BghU gedragscode elektronisch verkeer.

12.3 BEWUSTZIJN

Functionaris Gegevensbescherming en Security Officer (CISO) focussen zich op de bewustwording (awareness) voor een veilig gebruik van privacy gevoelige gegevens en het informatieveiligheid in het algemeen. Om het urgentiegevoel en het bewustzijn te vergroten, verzorgen ze (lunch)lezingen, bezoeken procesteams. De medewerker kan alle informatie vinden op intranet.

12.4 Informatie Beveiligings Dienst

De BghU is 'officieel' aangesloten bij de Informatie Beveiligings Dienst(IBD). De IBD is een gezamenlijk initiatief van de VNG Realisatie (voorheen KING). en is er voor alle gemeenten, samenwerkingsverbanden. De IBD richt zich op bewustwording, kennisdeling en concrete ondersteuning op het vlak van informatiebeveiliging (incidentpreventie, -detectie en -coördinatie). De IBD is voor gemeenten en samenwerkingsverbanden het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD beheert de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en geeft regelmatig kennisproducten uit.

Door aan te sluiten bij de IBD, krijgt de BghU specifieke ondersteuning op het vakgebied van informatiebeveiliging voor implementatie, beheer en in geval van beveiliginsaspecten.

Hoofdstuk 13. Vaststelling

Dit document is geactualiseerd onder regie van CISO S. Lee en ICT-beheerder J.D. de Jong en afgestemd met informatiemanager R.R. Dalebout.
Document is niet afgestemd met businesscontroler, deze functie is vacant.

Namens de directie van BghU,
voor akkoord:

Utrecht, 25 september 2018,

A.H. Geytenbeek,
directeur.

BIJLAGEN

BIJLAGE I OVERZICHT EXTERN BEHERENDE ORGANISATIES

Huisvesting hardware integraal belastingpakket (lights out centre)

Leverancier A

Beheer software integraal belastingpakket en BghU domein (op afstand)

Leverancier B

Netwerkbeheerder LAN BghU kantoor Utrecht

Leverancier B

Dataverbinding Utrecht en Gouda, beide externe partijen een rol.

Leverancier D

Leverancier E

MijnBghU

Leverancier F

BIJLAGE II PRIVACY GEGEVENS

Opsomming privacy gevoelige gegevens

Gegevens op MijnBghU	**Privacy gevoelig**
Geslacht man/vrouw	J
Achternaam	J
Voornamen	J
Adres	J
Huisnummer	J
Postcode	J
Woonplaats	J
Telefoonnummer	J
E-mail	J
Bankrekeningnummer	J
Machtiging tot automatische incasso J/N	N
BSN	J
Klantnummer	J
Openstaand saldo	J
Opgelegde aanslagen	J
Soort belasting	N
Grondslag	J
Tarief	N
Transacties met BghU	J
Foto's met herkenbaarheid van natuurlijke personen	J

BIJLAGE III GEHEIMHOUDINGSVERKLARING

Geheimhoudingsverklaring (externe) medewerkers

De BghU heeft als organisatie een voorbeeldfunctie in de maatschappij. Dit brengt voor externe medewerkers, werkzaam voor de BghU speciale verantwoordelijkheden met betrekking tot het omgaan met privacy gevoelige informatie met zich mee.

Deze verklaring heeft tot doel dat u zich hier bewust van bent en dat u belooft zich daarnaar te gedragen.

Gegevens (externe) medewerker :

Naam en voorletters :

Adres :

Woonplaats :

Werkzaam bij werkstroom :

Hiertoe verklaar ik het volgende:

Ik zal op een verantwoorde wijze op privacy gevoelige informatie omgaan. Dit betekent dat ik deze informatie alleen voor mijn werkzaamheden binnen de BghU zal gebruiken en niet met derden zal delen. Tevens heb ik kennis genomen van het Informatie BeveiligingsPlan BghU toegankelijk o.a. via BghU intranet en zal daar naar handelen.

Datum:

Handtekening (externe) medewerker:

BIJLAGE IV UITVOERINGSREGELING GEDRAGSCODE ELEKTRONISCH VERKEER

Artikel 1: Doel en uitgangspunten

a. Deze gedragscode bevat regels ten aanzien van verantwoord gebruik van online middelen zoals E-mail en internet en over de wijze waarop controle op persoonsgegevens over het gebruik van E-mail en internet plaatsvindt.

b. Deze gedragscode geldt ook voor het gebruik van offline middelen zoals telefoon.

c. Met het invoeren van de gedragscode wil de werkgever voorkomen:

    a. Dat het gebruik in strijd is met de openbare orde of goede zeden;

    b. Dat door het gebruik de goede naam van de BghU wordt aangetast;

    c. Dat door het gebruik de systeem- en netwerkbeveiliging in gevaar komt.

d. De privacy van de medewerker wordt gewaarborgd conform wet- en regelgeving.

e. Persoonsgegevens over E-mail en internetgebruik worden niet langer bewaard dan noodzakelijk, met een maximum bewaartermijn van 6 maanden.

f. Online middelen als internet en E-mail zijn, evenals offline middelen als telefoon, te beschouwen als bedrijfsmiddelen waaraan de werkgever ten aanzien van het gebruik ervan nadere regels kan stellen.

g. De in deze gedragscode gestelde regels hebben betrekking op goed werknemerschap.

h. De controle op Internet- en e-mailgebruik zal overeenkomstig deze gedragscode worden uitgevoerd. Indien er zich situaties voordoen waarin deze regeling niet voorziet, zal conform het arbeidsrechtelijk kader en de WBP en in overleg met de ondernemingsraad gehandeld worden.

Artikel 2: Begripsomschrijving

Medewerker:	een persoon werkzaam bij de BghU, in de hoedanigheid van ambtenaar, medewerker met een arbeidsovereenkomst, vakantiekracht, uitzendkracht of op andere wijze ingehuurd of tewerkgesteld door en/of bij de BghU;
Online middelen:	elektronische communicatie - en informatiemiddelen zoals E-mail en internet, die gebruikt kunnen worden met behulp van een systeemnetwerk en die tot doel hebben het uitoefenen van de functie te ondersteunen;

Offline middelen: communicatie - en informatiemiddelen zoals telefoon, die tot doel hebben het uitoefenen van de functie te ondersteunen en waarvoor geen systeemnetwerk nodig is;

Oneigenlijk gebruik: gebruik van E-mail of internet dat in strijd is met de gestelde gedragsregels (zie artikel 3 en 4).

Artikel 3: Gedragsregels E-mail

a. De medewerker hanteert in een E-mail gepast taalgebruik. Ook eventuele meegezonden documenten of beelden zijn gepast, dat wil zeggen niet in strijd met de openbare orde of goede zeden (zoals discriminerende en pornografische teksten en afbeeldingen).

b. De medewerker heeft toestemming het E-mailsysteem ook privé te gebruiken.
Om te voorkomen dat de goede naam van de BghU wordt aangetast geldt ook bij privé gebruik het gestelde in lid 3.a

c. Het is de medewerker niet toegestaan om via een E-mail software te versturen of te ontvangen. Indien (aanpassingen van) software door de medewerker wordt ontvangen, stuurt hij deze door naar ICT-beheer. Deze stelt vast of de software kan worden geïnstalleerd en draagt vervolgens zorg voor de verdere afwikkeling.

d. Het is de medewerker niet toegestaan ongeautoriseerd gebruik te maken van het E-mailsysteem, dan wel pogingen daartoe te ondernemen.

e. De werknemer is zich ervan bewust dat zijn mailbox in het kader van het bedrijfsbelang toegankelijk is voor werkgever en andere werknemers, waardoor het onontkoombaar is dat werkgever of andere werknemers de inhoud van de door hem of haar verzonden of ontvangen emails met een al dan niet zakelijk karakter toevalligerwijs kunnen waarnemen.
Werkgever staat het evenwel toe dat werknemer een eigen webbased emailaccount neemt, waarmee emails met een niet-zakelijk karakter worden verzonden of ontvangen, zodat hiermee ongewenste inzage in privacy gevoelige gegevens wordt voorkomen. Het gebruik van deze eigen emailaccount is eveneens onderworpen aan de regels van dit reglement.

Artikel 4: Gedragsregels internet

a. Het is de medewerker niet toegestaan op internet materiaal te benaderen, te verzamelen of beschikbaar te stellen dat in strijd is met de openbare orde of de goede zeden (zoals discriminerende en pornografische teksten en afbeeldingen).

b. De medewerker heeft toestemming internet privé te gebruiken. Het verbod zoals gesteld in lid 4.a is ook bij privé gebruik van toepassing.

c. Het is de medewerker toegestaan bestanden van internet te downloaden voor zakelijk gebruik.

d. Het is de medewerker toegestaan privé-bestanden op te slaan tot een maximum van 100 Mb met in achtneming van het gestelde in lid 1. Privé-bestanden die het maximum overschrijden dienen door de medewerker te worden verwijderd.

e. Het is de medewerker niet toegestaan ongeautoriseerd gebruik te maken van internet, dan wel pogingen daartoe te ondernemen. De BghU behoudt zich het recht voor bepaalde internetsites en -pagina's voor de medewerker te blokkeren, zodat de medewerker deze sites of pagina's niet kan bezoeken.

Artikel 5: Controle en maatregelen

a. Controle op het gebruik van E-mail en internet heeft alleen betrekking op de doelen, genoemd in artikel 1, lid c, sub a, b en c.

b. De informatiemanager of directie kan, indien gewenst, een ICT-beheerder verzoeken hem te rapporteren over het gebruik van E-mail en internet. Deze rapportage vindt plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot individuele medewerkers. Het is de ICT-beheerder die de rapportage verzorgt niet toegestaan om deze rapportage schriftelijk dan wel mondeling aan anderen dan de directie of informatiemanager te verstrekken.

c. Indien een ernstig vermoeden bestaat dat een medewerker of groep medewerkers de gedragsregels overtreedt kan, op verzoek van de directie, door een ICT-beheerder gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden.

d. De in lid c bedoelde controle beperkt zich in eerste instantie tot verkeersgegevens van het E-mail en internetgebruik. Slechts bij zwaarwegende redenen vindt controle op de inhoud plaats.

e. Bij constatering van verboden E-mail en internetgebruik wordt dit onmiddellijk door de leidinggevende met de medewerker of groep medewerkers besproken.

f. Overtredingen van de in deze gedragscode gestelde regels worden gezien als plichtsverzuim. Bij overtredingen kan directie dan ook (disciplinaire) maatregelen nemen. Tevens kan het gebruik van E-mail en internet voor de medewerker of groep medewerkers worden beperkt.

Artikel 6: De Ondernemingsraad

a. Leden van de Ondernemingsraad hebben het recht, op grond van artikel 17 van de Wet op de Ondernemingsraden, om vertrouwelijk te overleggen met gebruik van de voorzieningen van de werkgever. Het is de BghU niet toegestaan om kennis ten nemen van de E-mail van een medewerker in de functie van lid van de Ondernemingsraad, tenzij het vermoeden bestaat dat het gebruik in strijd is met de gestelde gedragsregels.

b. Voor de leden van de Ondernemingsraad zijn de gestelde gedragsregels ten aanzien van gebruik van E-mail en internet van overeenkomstige toepassing.

Artikel 7: Overige bepalingen

In individuele gevallen waarin deze gedragscode niet voorziet beslist de directeur indien daar naar zijn oordeel, op basis van redelijkheid en billijkheid, reden toe is.

Artikel 8: Inwerkingtreding

De gedragscode treedt in werking met op datum van ondertekening van dit document door directeur BghU.

BIJLAGE IV PROCEDURE MELDING EN AFHANDELING DATALEK

Deze procedure is een onderdeel van het BghU Informatie BeveiligingsPlan (IBP) en wordt minimaal eenmaal per jaar geactualiseerd.

INLEIDING

Dit document beschrijft de verschillende stappen die binnen BghU genomen worden bij een datalek, die valt onder de Meldplicht Datalekken. De meldplicht datalekken is een wijziging van de Wet Bescherming Persoonsgegevens, is in werking getreden met ingang van 1 januari 2016. Bij een datalek is er sprake van een inbreuk op de beveiliging van persoonsgegevens (als bedoeld in artikel 13 van WBP. De persoonsgegevens zijn dan blootgesteld aan verlies of onrechtmatige verwerking.

- Ter illustratie datalekken kunnen bij voorbeeld ontstaan door:
- moedwillig handelen (cybercriminaliteit, hacking, identiteitsfraude, mailware besmetting);
- technisch falen (ICT-storingen);
- menselijk falen (te eenvoudige wachtwoorden/het verstrekken van username/wachtwoord aan collega's en externen);
- calamiteit (brand datacentrum, wateroverlast);
- verloren USB stick of laptop;
- verzenden van E-mail bijlage met persoonsgegevens;
- maar ook het onrechtmatige (al dan niet geautomatiseerde) verwerking van gegevens.

Een datalek moet onverwijld (binnen 3 dagen) nadat de verantwoordelijke (1) binnen BghU er kennis van heeft genomen, bij de Autoriteit Persoonsgegevens (voormalig CBP) gemeld worden.

Het datalek moet ook worden gemeld bij de betrokkenen. In het geval van BghU zijn dit over het algemeen klanten (burgers en bedrijven) of medewerkers. Betrokkenen zijn degenen wiens persoonsgegevens zijn betrokken bij een inbreuk. De betrokkene moet onverwijld in kennis worden gesteld van de inbreuk, indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor zijn persoonlijke levenssfeer.

Een bewerker (2) is verplicht om een datalek te melden bij de verantwoordelijke.

1 Verantwoordelijke: directie BghU. De verantwoordelijke heeft zeggenschap over doel en wijze van verwerking. Formeel, juridisch en feitelijk degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. Degene die zeggenschap heeft en verantwoordelijk is over doel en middelen van verwerking en beslist over bewaartermijnen, verstrekking inzageverzoeken etc. De verantwoordelijke heeft de regierol;

2 Bewerker: degene die de gegevens ten behoeve van de verantwoordelijke verwerkt zonder aan zijn of haar rechtstreeks gezag te zijn onderworpen, ook extern. De bewerker verwerkt persoonsgegevens overeenkomstig de instructies en uiteindelijke verantwoordelijkheid van de verantwoordelijke. De bewerker neemt geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en andere ontvangers, de uur van de opslag van de gegevens etc.

MELDEN

Alle datalekken van persoonsgegevens moeten intern worden gemeld aan de Chief Information Security Officer (CISO) en worden gedocumenteerd in TopDesk. De melding registratie wordt door BghU ICT-beheerder gedaan. Het aanmelden kan ook door een externe persoon worden gedaan bij een willekeurige medewerker van BghU. De aanmelding moet direct persoonlijk of telefonisch/WhatsApp worden gedaan bij de Chief Information Security Officer (CISO) en in TopDesk in detail schriftelijk worden vastgelegd. IM meldt het datalek zo nodig bij de Autoriteit Persoonsgegevens. 24/7 alle dagen is de informatiemanager hiervoor telefonisch of via WhatsApp bereikbaar: in geval de Chief Information Security Officer (CISO) onverhoopt niet bereikbaar is neemt directielid rol CISO in dit kader over.

REGISTREREN:

- naam van de melder;
- datum en tijd van de melding;
- aard van de inbreuk (is er aanmerkelijk risico op verlies of onrechtmatige verwerking?);
- welke persoonsgegevens vallen onder de melding;
- om welk aantal en/of gegevensrecords gaat het;
- welke (groepen) personen zijn betrokken bij de melding;
- welke maatregelen zijn of worden door de melder getroffen;
- welke gevolgen zijn er volgens de melder voor de betrokkenen;
- de contactpersoon ICT-beheer voor de melding.

EERSTE ANALYSE

De Chief Information Security Officer (CISO) ondersteunt door ICT-beheerder(s) beoordelen of van de inbreuk 'redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijk risico op verlies of onrechtmatige verwerking, waaraan nadelige gevolgen voor de privacy van de betrokkenen zijn verbonden'. Is dit niet het geval, dan vindt alleen registratie van de melding plaats in TopDesk.

Is dit wel het geval, dan wordt de BghU directie ingelicht en een team van materiedeskundigen geformeerd (responseteam).

RESPONSETEAM DATALEK

In geval er sprake is van een datalek wordt met een hoogste prioriteit materiedeskundigen bijeengeroepen door de CISO. De bijeenkomst wordt voorgezeten door de CISO. Het responseteam bespreekt:

- de gegevens die zijn vastgelegd bij het aannemen van de melding.;
- de noodzakelijke vervolgacties m.b.t. het datalek (lek onmiddellijk dichten, toegang tot informatie beperken en tegelijkertijd meer informatie vergaren over de indringer;
- hetgeen gemeld gaat worden bij het Autoriteit Persoonsgegeven (AP)
- naast aard inbreuk, welke persoonsgegevens, aantal betrokken personen/records:
- de mogelijke gevolgen voor de betrokkenen;
- de maatregelen die BghU en/of bewerker neemt en/of kan nemen om de schade voor betrokkenen te verkleinen;
- de maatregelen die betrokkenen kunnen nemen om verdere schade te verkleinen, inclusief de wijze van inlichten hierover;
- contactgegevens voor betrokkenen;
- de wijze van afhandeling intern, inclusief communicatie naar melder, bewerkers en eigen organisatie.
- CISO bespreekt met directie casus: directie draagt zorg voor of het wel of niet inlichten bestuur(ders).
- of er sprake is van eigen aansprakelijkheid, of aansprakelijkheid van derden, zoals uit hoofde van wanprestatie (omdat een geheimhoudingsverplichting is geschonden, of in strijd met een contractuele verplichting onvoldoende beveiliging is gerealiseerd) of onrechtmatige daad;

- het al dan niet doen van aangifte en vaststellen of sprake is van strafrechtelijke verwijtbaarheid. Dit kan bijvoorbeeld spelen wanneer er sprake is van betrokkenheid vanuit BghU zelf, een bewerker, of wanneer er onvoldoende maatregelen zijn getroffen om ongeregeldheden te voorkomen. Indien gewenst vindt overleg plaats met de juridisch adviseur;
- hetgeen intern gecommuniceerd wordt, op welk moment;
- hetgeen extern gecommuniceerd wordt, op welk moment. Er wordt vastgesteld of de pers geïnformeerd moet worden;
- of naast het AP ook andere stakeholders geïnformeerd worden;
- of er individuen, bedrijven, gemeenten, waterschappen, VNG, Unie van Waterschappen geïnformeerd worden;
- op welke wijze er intern wordt gerapporteerd;
- of eventuele schade is gedekt door de verzekeringspolis.

INLICHTEN BGHU DIRECTIE

De CISO rapporteert aan de BghU directie de uitkomsten van het overleg van het Responseteam Datalek. De BghU directie accordeert de uit te voeren activiteiten, zoals vastgesteld door het Responseteam Datalek, of stelt de uit te voeren activiteiten bij. De door de BghU directie vastgestelde activiteiten worden uitgevoerd.

MELDING BIJ HET AUTORITEIT PERSOONSGEGEVENS

De CISO meldt datalek bij het AP

In ieder geval zal gemeld moeten worden:

- aard van de inbreuk, waaronder betrokken categorieën, aantal betrokkenen, aantal gegevensrecords;
- beschrijving van de te verwachten gevolgen;
- getroffen en/of voorgestelde maatregelen;
- informatie over te nemen maatregelen door de betrokkene om de nadelige gevolgen te beperken;
- contactgegevens voor betrokkene;

ONTVANGSTBEVESTIGING AUTORITEIT PERSOONSGEGEVENS

Is er een melding gedaan, dan ontvangt BghU een ontvangstbevestiging. Bij de meldingen die aanleiding geven tot nadere actie door het AP, zal het AP contact opnemen met BghU om de herkomst van de melding te verifiëren.