



Fysieke beveiliging UWV-locaties

Versie 2.0



Versiebeheer

Versie	Datum	Status	Korte beschrijving aanleiding/ wijziging
1.0	30-7-2019	Definitief	Vastgesteld in MT H&F op 30-7-2019
2.0	03-02-2021	Definitief	Tekstuele aanpassingen (BIO, instructies fysieke beveiliging per pand), verwijzing naar het register van verwerkingsactiviteiten van persoonsgegevens opgenomen.

Opgesteld door : Elkan van Dijk, Eric van Amsterdam
Versiebeheer : Monique van Blerk

Gerelateerde documenten

Document	Versie	Datum
BIO 2020		2020
BIR 2017		2017
UWV BIR 2014		2014
Tactisch beleid informatiebeveiliging en privacy		2015



Inhoud

1	Inleiding BIO	4
2	Verantwoordelijkheid Facilitair Bedrijf	5
3	Toegangsbeleid	6
4	Gebouw en inrichting	8
5	Technische beveiliging	11
6	Beveiligingsdiensten	13
7	Houding en gedrag	16
8	Organisatie beveiliging	18

1 Inleiding BIO

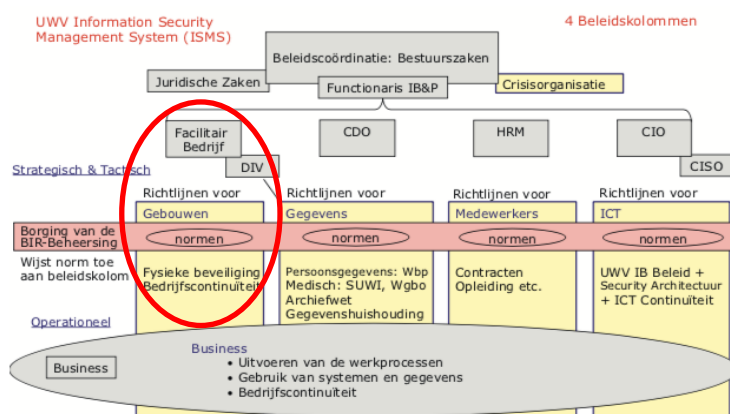
In dit document wordt uiteengezet op welke wijze de fysieke beveiliging binnen UWV is georganiseerd.

UWV kent als uitvoerder van de sociale werknemersverzekeringen een hoge mate van zichtbaarheid in Nederland. Haar positie binnen het sociale zekerheidsbestel vraagt om een zorgvuldige en goede behartiging van de verschillende belangen van de overheid, de sociale partners en de verzekerden. UWV is daarom een risicomijdende organisatie.

UWV is een informatieverwerker die de beschikking heeft over heel veel vertrouwelijke (persoons)gegevens. Vanuit deze context heeft de Raad van Bestuur besloten om als Zelfstandig BestuursOrgaan (ZBO) te voldoen aan de vereisten vanuit de Baseline Informatiebeveiliging Overheid, Tactisch Normen Kader (TNK), en aan te sluiten bij de wereld van open en breed geaccepteerde standaarden.

De onderstaande figuur vormt het uitgangspunt voor het benoemen van de Taken, Verantwoordelijkheden en Bevoegdheden (TVB) bij de UWV BIO-vereisten.

Governance Informatiebeveiliging en Privacy (IB&P)



Figuur 1: Fysieke (toegangs)beveiliging als onderdeel van IB&P

Het 'eigenaarschap' van een norm houdt in het dragen van de verantwoordelijkheid voor de norm en voor de realisatie van de onderliggende maatregelen. Een verantwoordelijkheid kan bij een of meer van de beleidskolommen zijn belegd. Gezien de vereiste consistentie tussen de onderlinge afhankelijkheden heeft UWV gekozen voor een integrale benadering van IB&P door centraal het document 'Borging van de BIR Beheersing' op te stellen.

De TVB's vormen de administratie van de 'Borging van de BIR Beheersing', welke door de CISO namens de CIO wordt onderhouden. In dit kader is de CIO niet de eigenaar van alle vereisten van de UWV BIR. De directeurs van de verschillende beleidskolommen zijn ieder verantwoordelijk binnen hun verantwoordelijkheidsgebied.

2 Verantwoordelijkheid Facilitair Bedrijf

In 2015 is het tactisch beleid informatiebeveiliging en privacy (sectie C versie 2.0) vastgesteld waarin de borging van de UWV BIR t.a.v. taken, verantwoordelijkheden en bevoegdheden is vastgelegd. Dit document vormt de basis van het IB&P-beleid en bevat het tactisch normenkader. Onderdeel van dit tactisch beleidskader is de fysieke beveiliging en de beveiliging van de omgeving, hiervoor is het Facilitair Bedrijf verantwoordelijk.

Het tactisch beleidskader betreft een normenkader welke uitgewerkt dient te zijn in onderliggend beleid, richtlijnen en instructies.

T.a.v. de fysieke beveiliging onderscheiden we de volgende zaken:

1. Toegangsbeleid
2. Gebouw en inrichting
3. Technische beveiliging (hard en software)
4. Dienstverlening beveiliging
5. Houding en gedrag

Werkingsgebied

De richtlijnen fysieke toegangsbeveiliging UWV zijn van toepassing op alle locaties, ruimtes en/of buitengebied waar UWV-huurder is en waar medewerkers en processen van het UWV structureel aanwezig zijn. Tevens zijn deze richtlijnen van toepassing op alle medewerkers, bezoekers, leveranciers en andere medegebruikers van de locaties van UWV.

Brondocumenten

De verschillende onderdelen m.b.t. fysieke beveiliging zijn op onderdelen nader uitgewerkt in verschillende brondocumenten. In onderstaande tabel zijn de brondocumenten beschreven waarin in dit document per paragraaf wordt verwezen.

#	Toelichting	Jaar	Beheer
1	BIO	2020	Overheid
2	BIR UWV	2014	CISO
3	Tactisch beleid informatiebeveiliging en privacy	2015	Bestuurszaken
4	Fysieke beveiliging UWV-locaties	2019	FB
5	Beleid sleutelplan	23-7-2014	FB
6	Functioneel programma van eisen inrichting	Maart 2017	FB
7	Technisch programma van eisen gebouwen		FB
8	Technisch programma van eisen geïntegreerd beveiligen		FB
9	Geïntegreerd beveiligen – analyse en ontwerp	21-2-2019	FB
10	Documenten fysieke beveiliging pand (voorheen Objectinstructies per locatie)	2020	FB
11	Protocol videomanagement	2019	FB
12	Agressieprotocol	2013	Bestuurszaken
13	Cleardesk policy	2013	Bestuurszaken
14	Huisregels en gedragsregels klantzone	2013	HRM
15	Functiebeschrijvingen multiservice leveranciers	2016	HRM

3 Toegangsbeleid

Ten behoeve van de fysieke beveiliging en de beveiliging van informatie is er toegangsbeleid voor alle UWV-locaties. Het toegangsbeleid spitst zich daarnaast toe op de fysieke beveiliging van kantoren, ruimten en faciliteiten. Onderstaand fysiek toegangsbeleid is als "good practice" voor de BIR 2017 geschreven door de Vereniging Nederlandse Gemeenten (VNG). Dit document is aangepast naar UWV.

Doel

Het doel van het beleid is:

1. Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie, bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten.
2. ICT-voorzieningen behoren fysiek te worden beschermd tegen toegang door onbevoegden, schade en storingen. ICT-voorzieningen die kritieke of gevoelige bedrijfsactiviteiten ondersteunen, behoren fysiek te worden ondergebracht in beveiligde ruimten, beschermd door afgegrensde beveiligde gebieden, in een gecontroleerde omgeving, beveiligd met geschikte beveiligingsbarrières en toegangsbeveiliging.
3. Het voorkomen van verlies, schade of diefstal van apparatuur en bescherming tegen fysieke bedreigingen en gevaren van buitenaf.

Uitgangspunten

UWV hanteert de volgende beleidsuitgangspunten:

1. UWV heeft barrières aangebracht om ruimten te beschermen waar zich ICT-voorzieningen dan wel persoonsgegevens (art. 4 AVG) en/of gevoelige gegevens bevinden (classificatie).
2. Er is een zoneringsplan met daarin opgenomen de volgende zones: Openbaar, wachtruimten en spreekkamers, werkruimten, ICT-ruimte/beveiligde ruimte (paspoort opslag of persoons- of gevoelige gegevens) en een off-site back-up locatie.
3. Er is een overvalplan met afspraken over aanrijroutes en contacten met de politie.
4. Er is cameratoezicht op toegangswegen en beveiligde ruimtes.
5. Gebouwen bieden voldoende weerstand bij gewelddadige aanvallen zoals inbraak en vandalisme, hierbij wordt ook rekening gehouden met de omgeving.
6. Er zijn alarmknoppen geplaatst in wachtruimten en spreekkamers en op verder alle plaatsen waar bezoekers in contact komen met UWV-medewerkers.
7. De kwaliteit van de toegangsmiddelen hoort in overeenstemming te zijn met de zonering.
8. Toegang tot gebouwen of beveiligingszones is alleen mogelijk na autorisatie.
9. Voor toegang tot speciale ruimtes is doelbinding vereist ((ICT)-Beheer, BHV, BRP, PUN). Toegang tot deze ruimtes wordt middels logging vastgelegd. De toegangslijsten worden periodiek gecontroleerd.
10. In gebouwen met beveiligde zones houdt beveiligingspersoneel toezicht op de toegang en houdt hiervan een registratie bij.
11. Er is 24 uur, 7 dagen per week bewaking met een inbraak alarm gekoppeld aan een alarmcentrale. Voor alle medewerkers die autorisatie hebben om het alarm te

bedienen dient een persoonlijke code gebruikt te worden; er wordt geen gebruik gemaakt van een generieke code.

12. Medewerkers/bezoekers zonder autorisatie mogen alleen onder begeleiding van bevoegd personeel en als er een noodzaak is, toegang krijgen tot de beveiligde omgeving.
13. Zonder expliciete toestemming mogen in beveiligde ruimtes geen opnames (beeld en/of geluid) worden gemaakt.
14. Niet uitgegeven toegangsmiddelen worden beveiligd opgeborgen.
15. Toegangsmiddelen vallen onder de verantwoordelijkheid van HRM/ de facilitaire dienst.
16. Er vindt één keer per half jaar een controle/evaluatie plaats op de autorisaties voor fysieke toegang. Voor speciale toegangsrechten is dat minimaal ieder kwartaal.
17. De huisregels voor toegangsbeleid worden bekend gesteld aan al het personeel en de bezoekers.
18. Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, zijn beheerst en afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te vermijden.

Verschillen per locatie

De in deze rapportage beschreven richtlijnen zijn de richtinggevende kaders, in de praktijk kan het voorkomen dat een locatie (nog) niet voldoet aan deze kaders. Hieronder wordt kort uiteengezet waarom een beleidswijziging niet altijd in één keer doorgevoerd kan worden en waarom er verschillen tussen vestigingen kunnen zijn:

1. UWV opereert in een dynamische omgeving. Wijzigingen van wet- en regelgeving of koerswijzigingen voordoen die effecten hebben voor de organisatie, vastgoed of inrichting kunnen niet van de ene op andere dag geïmplementeerd worden.
2. Veranderingen in een vestigingen netwerk kost vele jaren, gezien lopende contracten, hoge investeringen en boekwaardes. Investeringswijzigingen zullen derhalve doorgaans op logische momenten worden doorgevoerd.
3. UWV kent geen eenduidig netwerk van vestigingen. Er komen meerder combinaties voor tussen front- en backoffice (fontoffice-SMZ, WERKbedrijf, backoffice – Uitkeren, Bezwaar en Beroep, Handhaven). In een aantal gevallen is UWV ook gevestigd bij een gemeente.
4. De implementatie van aanbestedingen hebben soms een lange doorlooptijd vanwege de complexiteit en (des)investeringen. Tijdens deze implementatietijd ontstaat er een hybride situatie van een "oude" en "nieuwe" omgeving.

4 Gebouw en inrichting

In dit hoofdstuk worden op hoofdlijnen de relevante zaken besproken t.a.v. gebouw en inrichting. Nadere informatie is te vinden in de brondocumenten.

Programma's van eisen

In het functioneel en technisch programma van eisen van UWV zijn de kaders opgenomen t.b.v. de inrichting van de UWV-kantooromgeving. Het hebben van UWV brede kaders voor de inrichting van gebouwen die aansluiten bij het werkproces is van groot belang. Ze geven richting aan het inrichtingsproces en draagvlak bij gebruikers. Ze zijn zowel sturend voor de indeling van het gebouw en het gebruik van de ruimte.

De programma's van eisen over de inrichtingsconcepten komen tot stand in overleg met de betreffende divisies. Besluitvorming hierover vindt plaats via de lijn divisie, Raad van Bestuur en advies van de Ondernemingsraad (indien van toepassing).

Ten aanzien van de fysieke beveiliging van het gebouw en de inrichting ervan zijn de volgende uitgangspunten op hoofdlijnen van belang.

Uitgangspunten

Ten aanzien van de fysieke beveiliging zijn de navolgende uitgangspunten van toepassing:

1. Fysieke pandbeveiliging: naast de inzet van beveiligingsmedewerkers zijn bouwkundige en elektronische maatregelen aanwezig voor het beveiligen van de UWV-locaties. Er is een 24/7 bewaking van de locaties van UWV, waarbij een inbraakalarm gekoppeld aan een alarmcentrale het minimum is conform UWV BIR 2017.
2. Zoneringsconcept: UWV hanteert een zonering bij alle locaties. Per zonering worden specifieke toegangsrechten toegekend. Iedere UWV-medewerker¹ heeft toegangsrechten tot zone 1 en 2. Voor zone 3 worden rechten uitsluitend toegekend op basis van doelbinding. Voor klanten gelden andere toegangsregelingen (zone 0). De navolgende zones zijn van toepassing:

Zone	Omschrijving	Voorbeelden	Toegangsrechten
0	Openbare zone	Openbaar buitenterrein	Iedereen
1	Publiekstoegankelijke zone (klantzone)	Receptie/balie/wachtruimte	Alle stakeholders van de organisatie
2	Interne, vertrouwelijke zone (werkzone)	Standaard werkplekken van de medewerkers	Eigen medewerkers en specifieke bezoekers
3	Strikt vertrouwelijke zone	Rekencentrum, MER/SER-ruimtes	Specifiek toegangsrecht

Tabel 2: Zoneringsconcept

¹ En gelijkgestelden (niet-UWV-medewerkers die op inhuurbasis in dienst zijn bij/voor UWV zoals ZZP'ers, uitzendkrachten, etc. Zij krijgen echter alleen toegang tot hun standplaats, niet tot alle UWV-locaties).

3. Principe van minimale toegang: personen krijgen uitsluitend toegang tot die zones, die hij/zij nodig heeft voor het uitvoeren van zijn/haar taken. Aan de hand van de rol van de persoon wordt de rechten voor toegang toegekend.
4. Toegang uitsluitend via UWV-toegangspas: toegang tot UWV-locaties kan uitsluitend worden verkregen via een UWV-toegangspas. Toegangspassen worden op de persoon verstrekt.
 - Klanten wordt alleen toegang verleend voor de publiekstoegankelijke zone, nadat is geverifieerd dat er een legitieme grond is voor een bezoek. Zij krijgen geen toegangspas;
 - Aan bezoekers wordt alleen toegang verleend nadat zij zich hebben gemeld bij receptie en ID-verificatie heeft plaatsgevonden. Zij ontvangen een toegangspas met een afwijkende kleur en dienen deze zichtbaar te dragen. Toegang tot de interne, vertrouwelijke zone kan alleen onder begeleiding van een medewerker van UWV (gastheer/gastvrouw). Deze gastheer/gastvrouw² is verantwoordelijk voor deze bezoeker.
 - Voor leveranciers, voor wie toegang tot het werkgebied gewenst is (vb. technisch onderhoud), kan het wenselijk zijn om deze zonder begeleiding toegang te verlenen. Leveranciers die structureel een pand bezoeken krijgen eveneens een pas een afwijkende kleur (anders dan die van bezoekers). In dat geval blijft gastheer/gastvrouw van UWV wel verantwoordelijk voor afspraken over toegang en controle hierop. De leveranciers dienen hun toegangspassen ook zichtbaar te dragen, zodat zij herkenbaar blijven als bezoeker.
5. Veiligheid informatie: de privacygegevens die verwerkt worden in het toegangscontrole- en cardmanagementsysteem en andere facilitaire systemen zijn afdoende beveiligd tegen misbruik en/of diefstal conform de nieuwe AVG-wetgeving.

Bezoekers

Bij de locaties van UWV dienen alle bezoekers (klanten en/of zakelijk bezoek), zich te melden bij de receptie. De beveiliging van de locaties dient zo te zijn ingericht dat een bezoeker niet zelfstandig de werkgebieden (2) en andere afgeschermd gebieden (3) kan binnengaan.

Werknemersingangen, nooddeuren, laad- en loslocaties

Eventuele werknemersingangen, nooddeuren, laad- en loslocaties dienen voldoende te zijn afgeschermd. Dit dient te gebeuren door middel van paslezers en eventueel een aanbelmogelijkheid. In het laatste geval zal een medewerker van UWV/security toegang verschaffen. Tevens is het van belang dat medewerkers van UWV geen bezoekers laten meelopen ("tail surfen"), indien zij zichzelf toegang verschaffen tot een gebied.

Informatieveiligheid

Archief ruimtes en serverruimtes vallen onder het "strikt vertrouwelijke gebied" (zone 3) en hebben extra beveiligingsmaatregelen, zoals beveiligd deurbeslag en kaartsloten met

² De gastheer/gastvrouw is de medewerk(st)er van UWV voor wie het bezoek komt.

toegangsregistratie. Daarbij bevinden deze serverruimtes zich bij voorkeur niet op de begane grond.

Veiligheid werkplekken klantzone

In de klantzone wordt bij de inrichting rekening gehouden met veiligheidsaspecten zoals:

- Indeling ruimte (bezoekers bij de ingang)
- Vluchtdeur
- Geen losse elementen
- Kleurgebruik
- Noodknop onder de bureaus met signaal naar beveiliging
- Videomonitoring
- Huisregels

Multi tenant situaties

UWV heeft te maken met werklocaties die facilitair niet onder de eigen verantwoordelijkheid vallen. Dit zijn bijvoorbeeld locaties waarbij het WERKbedrijf is gevestigd binnen een locatie van een gemeente, of een onderdeel van UWV binnen een kantoorverzamelgebouw.

Wanneer UWV in een gebouw is gehuisvest met meerdere huurders zullen alle toegangen/aangrenzende gebieden naar UWV in zone 2 en 3 beveiligd en voorzien van een toegangscontrolesysteem zijn.

Op enkele locaties wordt gebruik gemaakt van een lokaal TCS, hiervoor heeft de UWV-medewerker een andere (niet UWV) toegangspas nodig. Voor toegang tot een UWV-locatie geldt dat toegang alleen mogelijk is via een UWV-toegangspas. Voor UWV blijft de eis voor 100% toegangscontrole en registratie op de locaties van kracht. Indien dit echter gezien de lokale situatie niet mogelijk blijkt, dan kan alleen met goedkeuring van de directie hiervan worden afgeweken.

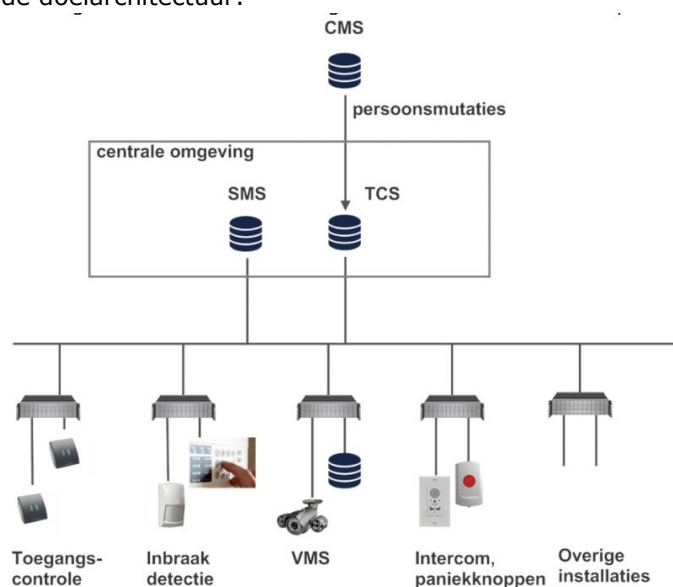
5 Technische beveiliging

In dit hoofdstuk worden op hoofdlijnen de relevante zaken besproken t.a.v. technische beveiliging. Nadere informatie is te vinden in de brondocumenten.

Nieuw security managementsysteem

Om de veiligheid van UWV-medewerkers en klanten te kunnen garanderen, wordt er geïnvesteerd in nieuwe veilige systemen en technologieën. Veel van deze beveiligingssystemen van UWV werken nu namelijk nog standalone op één locatie.

Met het project *geïntegreerde beveiliging* is het de bedoeling dat er één enkel platform wordt ontwikkeld voor alle UWV-locaties in de vorm van een nieuw security managementsysteem (SMS), dat bovendien op afstand benaderbaar is. Het volgende schema is een weergave van de doelarchitectuur:



Project geïntegreerde beveiliging UWV

Doelstelling is te komen een geïntegreerd beveiligingssysteem met de daarbij behorende dienstverlening door de introductie van een toekomst vaste systeemarchitectuur, waarbij rechtmatigheid, doelmatigheid, kwaliteitsverbetering op de systemen, een verhoging van de kwaliteit van de dienstverlening, optimale ondersteuning van de eigen processen. De scope betreft:

- Security Management System (SMS);
- Inbraak signaleringsinstallatie (INB)
- Toegangscontrolesysteem (TCS);
- Video Management Systeem (VMS);
- Paniekknoppen (PAN)/Assistent knoppen (ASS);
- Intercominstallatie (INT);
- Personen telling (PER).
- Personen zoek installatie (PZI).

Doelarchitectuur

De systemen dienen centraal te worden opgezet. Een centrale omgeving waarbinnen het SMS en het TCS zijn opgenomen. Op de locaties wordt geen software geïnstalleerd met uitzondering van videobeelden opname. Hierdoor worden flexibiliteit qua huisvesting, schaalbaarheid en effectief beheer mogelijk. De in te zetten systemen dienen minimaal op de volgende assen een kwaliteitsverbetering te realiseren:

Veiligheid

De systemen dienen het principe van end-to-end security te bevatten (design by security), Rijkspace compatibel sleutelmanagement te ondersteunen en een hoge mate van robuustheid te vertonen tegen cybercriminaliteit.

Modulariteit

De systemen dienen modulair te zijn opgezet met standaard interfaces met het oog op uitwisselbaarheid en schaalbaarheid.

Functioneel gebruik

De diverse gebruikers dienen door de systemen optimaal in hun taken ondersteund te worden.

Toekomstvastheid

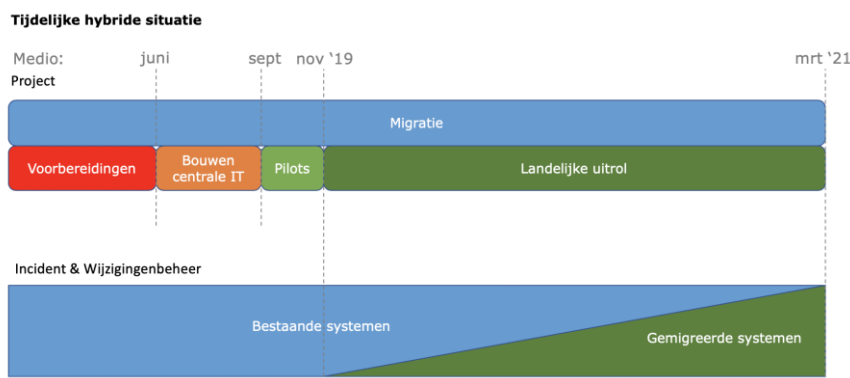
De ingezette technologie dient te zijn gebaseerd op moderne en toekomst vaste principes, zoals web-technologie en IP-gebaseerde hardware/componenten.

Scope toegangscontrole

Met toegangscontrole wordt expliciet de toegang voor personen tot UWV-locaties bedoeld en niet de toegang tot netwerken en systemen (toegangspoorten waaronder USB, Netwerk sockets en Wifi-netwerken) die in de kantoren van UWV aanwezig zijn.

Transitieproces

Gedurende het migratie project hebben we te maken met hybride situatie van huidige systemen en de gemigreerde systemen. In onderstaande grafiek is de migratieplanning op hoofdlijnen weergegeven.



6 Beveiligingsdiensten

In dit hoofdstuk worden de relevante zaken besproken t.a.v. de beveiligingsdiensten die ingekocht worden. Nadere informatie is te vinden in de brondocumenten.

Multi service leveranciers

UWV heeft haar uitvoerende werkzaamheden op het gebied van receptie en beveiliging uitbesteed aan twee multi serviceleveranciers (het land is verdeeld in Noord en Zuid). Deze leveranciers leveren ook diensten op het gebied van restauratieve voorzieningen, tuinonderhoud, schoonmaak, BHV, etc. UWV Facilitair Bedrijf voert de regio op de uitvoering.

Fysieke beveiliging per pand

Om richting te geven aan de uitvoering zijn per locatie fysieke beveiligingsinstructies gemaakt waarin de uitvoerende werkzaamheden op het gebied van beveiliging en veiligheid zijn beschreven. Het document 'fysieke beveiliging per pand' wordt jaarlijks geactualiseerd en vormt een naslagwerk voor de medewerkers lokaal.

Medewerkers van de leveranciers, werkzaam op een locatie waar deze instructies betrekking op hebben, zijn verplicht kennis te nemen van de inhoud van het document 'fysieke beveiliging per pand'. De instructies hebben tot doel deze medewerkers een taakomschrijving te geven, waarin onder meer hun bevoegdheden en verantwoordelijkheden tot uitdrukking komen.

Kaders aanbesteding

In onderstaande paragrafen zijn de teksten weergegeven zoals ze zijn opgenomen in de aanbesteding, als zodanig zijn de richtinggevend voor de te verlenen dienstverlening op het gebied van fysieke veiligheid. De teksten bestaan enerzijds uit een beleidskader over klantbenadering (A) en anderzijds een beschrijving van de dienstverlening (B) die door de mantelleveranciers geleverd wordt.

A - klantbenadering

Op de UWV-locaties komen klanten, leveranciers en personeel. Ieder heeft zijn eigen verwachtingen over de ontvangst aan de balie en baliepersoneel moet hieraan voldoen. Voor de klant is het beschreven baliebeleid leidend. Dat is getoetst aan de klantprincipes. Het beschreven baliebeleid is ook van toepassing op leveranciers. Voor UWV is het veiligheidsaspect een extra dimensie dat hieraan wordt toegevoegd.

Doelstellingen

Uitgangspunt zijn de veiligheidsprincipes Veilig en Vriendelijk: de klant ervaart de dienstverlening als maatwerk en de klant weet waar hij aan toe is. Om dit beleid te bereiken zijn de volgende doelstellingen gedefinieerd:

- Een complete beleving van veiligheid en toegankelijkheid waarbij klantgericht wordt zorggedragen voor een gastvrije en professionele ontvangst en het (pro) actief realiseren van een veilige werkomgeving. Het resultaat moet zijn dat de klant tevreden geïnformeerd vertrekt.
- Daar waar incidenten dreigen (te ontstaan) worden deze op professionele wijze voorkomen.
- Er is respect voor de klant; de klant is welkom en wordt als gast ontvangen en behandeld.

- Het bieden van een veilige omgeving in en nabij de entree/klantzone voor medewerkers en klanten waarbij noodzakelijke veiligheidsmaatregelen zijn getroffen (conform ARBO wet).
- Het waarborgen van de ongestoorde voortgang van de bedrijfsprocessen door middel van beveiligingsmaatregelen.
- Bescherming van (im)materiële eigendommen van UWV.

Uitgangspunten

UWV heeft kernwaarden geformuleerd voor haar bedrijfsprocessen. Dit zijn bereikbaarheid, persoonlijke aandacht, maatwerk, tijdigheid en duidelijkheid. Op basis hiervan is het dienstverleningsbeleid van UWV geformuleerd. Leidend hierbij zijn voor de ontvangst van klanten de principes persoonlijke aandacht, bereikbaar- en toegankelijkheid, in veiligheidstermen Veilig en Vriendelijk.

De visie van UWV Werken aan Perspectief: goed en snel geholpen klanten wordt in dit beleid verder uitgewerkt.

Klantprincipes

De ambities van UWV op het gebied van dienstverlening vertalen zich in een vijftal klantprincipes. Deze vijf klantprincipes zijn leidend bij het ontwerp, de inrichting én de uitvoering van onze dienstverlening. De vijf klantprincipes zijn:

1. UWV is goed bereikbaar en toegankelijk
2. UWV geeft persoonlijke aandacht
3. UWV levert maatwerk
4. UWV is tijdig in haar dienstverlening
5. UWV is duidelijk in wat de klant mag verwachten

B - Dienstverlening multi service leveranciers

Onderstaande tekst is een weergave van de aanbestedingsstukken t.a.v. beveiliging.

UWV heeft als doelstelling, een complete beleving van veiligheid en toegankelijkheid, waarbij klantgericht wordt zorggedragen voor een gastvrije en professionele ontvangst en een veilige (werk)omgeving. Opdrachtnemer levert de volgende diensten op basis van maatwerk per locatie.

Beveiligingsdiensten

- Opdrachtnemer levert het volgende complete pakket van beveiligingsdiensten:
- Vaste dienstverlening: inzet van security host, receptionisten met beveiligingstaken, gastheer-/gastvrouw, beveiligers en receptiemedewerker op UWV-locaties; Centralist (op het Hoofdkantoor van UWV); Dienstverlening op afroep; Open-, brand en sluitronden; Mobiele surveillance; Alarmopvolging; Meldkamerabonnement; Particuliere Alarm Centrale.
- Opleiding, training en/of instructie van het leidinggevende en uitvoerende personeel zijn voor rekening van Opdrachtnemer.
- Inschrijver maakt voor opleidingsplaatsen uitsluitend gebruik van door ECABO erkend
- Leerlingen mogen als extra capaciteit meelopen met gekwalificeerd personeel onder begeleiding van een coach, niet zijnde een ingeroosterde medewerker, en alleen na overleg met en goedkeuring door UWV. De kosten hieraan verbonden komen voor rekening van Opdrachtnemer.

Dienstverlening

- Opdrachtnemer verzorgt dagelijks een digitale registratie en rapportage betreffende de uitvoering van de werkzaamheden en de eventueel gesignaleerde bijzonderheden en genomen maatregelen.
- Opdrachtnemer biedt UWV web-based toegang tot het digitale registratiesysteem van Inschrijver om op vestiging- en districtsniveau inzicht te krijgen over incidenten en de afhandeling daarvan.
- Opdrachtnemer: verzorgt per locatie objectinstructies.
- Na gunning verzorgt Opdrachtgever de UWV-specifieke procedures inzake omgaan met lokaalverboden en het agressiebeleid van UWV. De objectinstructies blijven intellectueel eigendom van UWV
- Opdrachtnemer dient ervoor te zorgen dat te allen tijde een volledige bezetting, overeenkomstig de afgesproken tijdstippen, wordt gegarandeerd en is derhalve verantwoordelijk voor het kwantitatief op peil houden van de continuïteit van dienstverlening en de bezetting van het personeelsbestand, inclusief een vaste pool van medewerkers van Inschrijver. Tussen medewerkers zullen minimaal overdrachtsmomenten plaats vinden. Structurele vervanging van en nieuwe medewerkers uit de pool dient te worden afgestemd en overeengekomen met UWV.
- Opvolgtijden - Opdrachtnemer zorgt voor een snelle alarmopvolging en hanteert minimaal de volgende opvolgtijden:
 - o In 80% van de meldingen is de mobiele surveillance binnen 20 minuten aanwezig op de betreffende locatie;
 - o In 100% van de meldingen is de mobiele surveillance binnen 30 minuten aanwezig op de betreffende locatie.

Portofoons

- Binnen UWV wordt gebruik gemaakt van diverse soorten portofoons. Deze portofoons zijn eigendom van UWV.
- Opdrachtnemer is verantwoordelijk voor: Het leveren en repareren van de portofoons en bijbehorende accessoires; Het aanvragen van vergunningen bij Agentschap Telecom (voor deze dienst wordt eenmalig een machtiging afgegeven aan de leverancier);
- Levertermijnen - Levering nieuwe portofoons, binnen 5 werkdagen na bestelling;
- Aanvragen vergunningen bij Agentschap Telecom: binnen 5 werkdagen na aanvraag; Programmeren van toegekende frequenties en omprogrammeren: binnen 5 werkdagen na aanvraag; Offertes: reactietermijn binnen 5 werkdagen na aanvraag.

7 Houding en gedrag

In dit hoofdstuk worden op hoofdlijnen de relevante zaken besproken t.a.v. houding en gedrag. Nadere informatie is te vinden in de brondocumenten.

Inleiding

Fysieke beveiliging heeft ook te maken met houding en gedrag van medewerkers, bezoekers en leveranciers. Om richting te geven aan het gewenste houding en gedrag zijn er enkele UWV brede protocollen/ richtlijnen opgesteld die gelden voor alle locaties, medewerkers, bezoekers en leveranciers. De documenten worden hierna op hoofdlijnen toegelicht.

Agressieprotocol

De Raad van Bestuur van UWV draagt zorgt voor de veiligheid en het welbevinden van haar medewerkers, maar ook van cliënten en bezoekers van UWV-locaties. De Raad van Bestuur ziet het als haar taak een werkklimaat te scheppen waarin respect bestaat voor de persoonlijke integriteit van haar medewerkers. Dit betekent dat we geen enkele vorm van ongewenst gedrag, zoals agressie en geweld, tolereren.

Ter bescherming van haar medewerkers hanteert UWV een Agressieprotocol. In dit protocol worden de afspraken beschreven die binnen UWV van toepassing zijn ten aanzien van het voorkomen van agressie, het hanteren van agressie en de maatregelen die UWV neemt als een cliënt zich agressief gedraagt.

Verbaal of fysiek agressief gedrag wordt niet geaccepteerd. Als een cliënt of bezoeker zich agressief gedraagt wordt dat direct gemeld en geregistreerd. Bij voortdurende of ernstige vormen van agressie wordt melding of aangifte bij de politie gedaan.

Huisregels UWV-panden

Ten behoeve van medewerkers en bezoekers zijn huisregels opgesteld welke op een duidelijke plaats in de klantzone opgehangen zijn. Iedereen dient zich te houden aan deze huisregels.

Protocol videomanagement

Videocameratoezicht – door middel van zichtbare camera's – vindt alleen plaats op voor publiek toegankelijke ruimtes, te weten: ontvangstbalie, beursvloer, spreekkamers en daar waar cliënten toegang hebben tot niet afgesloten kantoorruimten. Er zullen geen camera's zijn in besloten ruimtes waar arbeid wordt verricht en op plaatsen waar medewerkers ongestoord zichzelf kunnen zijn. Alle medewerkers zullen worden geïnformeerd over de

aanwezigheid van camera's en het vastleggen van de opnames. Er zullen alleen beelden worden vastgelegd. Er worden geen geluidsopnamen gemaakt.

Beelden waarop individuen zijn te herkennen, kunnen worden aangemerkt als persoonsgegevens. Daarom valt cameratoezicht onder de werking van de Algemene verordening gegevensbescherming (AVG).

Er is een Videocameratoezichtprotocol opgesteld waarin wordt aangegeven hoe UWV VCT kan en moet inzetten binnen de wettelijke kaders en de kaders van de fysieke beveiliging.

Cleardesk policy

UWV heeft een cleardesk policy opgesteld. De naleving en controle daarop is een lijnverantwoordelijkheid. Iedere divisie dient dit zelf te organiseren. De inhoud van de policy is op hoofdlijnen als volgt.

Inhoud

Alle vertrouwelijke informatie moet na werktijd veilig worden opgeborgen. Dit gaat zowel om fysieke informatie, zoals dossiermappen en uitgeprinte stukken als om digitale informatie op je pc en in de printer.

Indien de cleardesk policy niet wordt nageleefd kan informatie in verkeerde handen vallen. Dat kan slechte gevolgen hebben voor klanten en medewerkers van UWV.

De cleardesk policy bestaat uit de volgende aanbevelingen:

1. Berg vertrouwelijke informatie na werktijd veilig op in afgesloten kasten/laden
2. Gebruik de pincode op de printer
3. Gebruik een pincode op je locker
4. Sluit je PC af na werktijd
5. Hou je wachtwoorden geheim
6. Verwijder vertrouwelijke informatie van whiteboards en flip-overs

8 Organisatie beveiliging

In dit hoofdstuk worden op hoofdlijnen de relevante zaken besproken t.a.v. organisatie en verantwoordelijkheden voor de fysieke beveiliging op de UWV-locaties.

Organisatie en verantwoordelijkheden

De directie van het Facilitair Bedrijf is binnen UWV onder andere verantwoordelijk voor de fysieke beveiliging van de locaties. Facilitair Bedrijf draagt zorg voor de uitvoering van de richtlijnen binnen de gestelde kaders. Hiervoor zijn lijnmanagers aangesteld die deze richtlijnen dienen te implementeren en uit te voeren. De overige divisies binnen UWV zijn gebruikers en dienen de richtlijnen na te leven. De uitvoering van beveiligingsdiensten zijn uitbesteed, UWV voert de regie op het beleid en de werkzaamheden.

In tabel 2 worden in algemene zin de verantwoordelijkheden toegelicht en aangegeven op welke wijze de evaluatie en bijstelling (PDCA) georganiseerd is.

Wie	Plan	Do	Check	Act
Directie dagelijkse uitvoering FB	Ontwikkelen van kaders (richtlijnen) en reglementen, meerjarenplannen.	Inbedden (landelijke) richtlijnen, adviseren, handreikingen.	Toeziën op naleving & actualisatie richtlijnen.	Bijsturen, opdracht-verstrekking voor verbeteracties en rapportage aan Raad van bestuur.
Manager facilitair en beheer	Formuleren van beveiligingseisen (classificatie) en opstellen clusterbeleid en beveiligingsplannen.	Stimuleren van beveiligings-bewustzijn bij medewerkers, uitvoeren risicoanalyses en bedrijfscontinuïteit-management.	Interne controle (IC), sturen op naleving van regels door medewerkers (gedrag), Naleving wetgeving.	Verbeteren bedrijfscontinuïteit Rapportage aan Directie.
Facilitair Manager	Beleidsvoorbereiding en vaststelling.	Leveren van security management systemen en services, incidentbeheer, logging, monitoring en advies.	Kwetsbaarheidsanalyse, evaluatie en rapportage.	Uitvoeren verbeteracties. Advies aan de staf over aanpassingen aan de beveiliging en doorvoeren van deze verbeteringen.
Gebruikers	Bekend zijn met de richtlijnen.	Naleven van de richtlijnen.		³

Tabel 2. Weergave van verantwoordelijkheden en wijze van evaluatie en bijstelling.

Incidentregistratie en -analyse

³ Eind 2020 is binnen Huisvesting en Facilitair een pilot gestart met een gewijzigde inrichting. Als de pilot succesvol is en de inrichting in 2021 formeel wijzigt, zal de rol van manager facilitair en beheer worden uitgevoerd door de regiomanager.

In de UWV BIR 2014 wordt beschreven dat van alle medewerkers, ingehuurd personeel en gebruikers van de faciliteiten van UWV wordt geëist dat zij alle waargenomen of verdachte zwakke plekken registreren en rapporteren bij de Facilitair Manager. De Facilitair Manager draagt er zorg voor dat beveiligings- en veiligheidsincidenten worden geregistreerd en periodiek worden geanalyseerd.

Evaluatie en audits

De opzet, het bestaan en de werking van de fysieke beveiliging worden periodiek geëvalueerd op basis van interne controles (bijv. mystery visits), externe audits en servicelevel rapportages geleverd door derden. Interne controles worden uitgevoerd door de lijnorganisatie. De bevindingen en aanbevelingen worden tussen de partijen onderling afgestemd en opgevolgd. Op basis van de bevindingen in de audit wordt dit document geactualiseerd.

Privacy

Binnen het domein "fysieke toegangsbeveiliging" worden verschillende persoonsgegevens verwerkt (bezoekersregistraties, camerabeelden, etc.). Bij het opstellen of wijzigen van procesbeschrijvingen en informatiesysteemdefinities binnen dit domein wordt steeds nagegaan of verwerking van persoonsgegevens aan de orde is of wijzigt en wordt ervoor gezorgd dat de wet- en regelgeving vanuit de BIO en AVG wordt nageleefd. Verwerkingen worden, zoals voorgeschreven in artikel 30 van de AVG, opgenomen in het register van verwerkingsactiviteiten van persoonsgegevens.