

Procedure Toegang Computerruimtes IDC/A

Versie 5.1

Inhoudsopgave

1	INLEIDING	2
1.1	Doel en scope van de procedure	2
1.2	Rollen	2
2	AUTORISATIEPROCEDURE	5
2.1	Aanmaak nieuwe passen	5
3.	PROCEDURE VERZOEK OM TOEGANG	6
3.1	Algemeen	6
3.1.1	Werkzaamheden in de kast van een andere partij	6
3.2	Registratie van legitimatiebewijs	7
3.3	Beschrijving procedure verzoek om toegang	7
4	TOEGANG BUITEN KANTOORTIJD	8
4.1	Procedure	8
5	PROCEDURE OPVRAGEN TOEGANGSLIJSTEN EN CAMERABEELDEN	9
5.1	Rapportage	9
6	NOODPROCEDURE	10
7	BEVEILIGINGSINCIDENTEN	11
8	RICHTLIJNEN	12
8.1	Gedragsregels voor het werken in computerruimtes	12
9	FUNCTIE- & CONTACTPERSONENLIJST	14
BIJLAGE 1:		15

1 Inleiding

1.1 Doel en scope van de procedure

De Computerruimtes worden door het IDC/A gezien als zeer kritische ruimtes. Dit betekent dat eventuele schade toegebracht aan deze ruimtes, van invloed kan zijn op een groot aantal kritische processen en systemen, vandaar dat het IDC/A de mogelijke kans wil minimaliseren. Onder Computerruimtes verstaan we het Datacenter Leyweg, MER-, SER- en overige technische ruimtes van het IDC/A. Fysieke toegang tot het CCH valt niet onder deze procedure. Deze ruimtes zijn verder gespecificeerd in bijlage 1.

Doel van deze procedure is het vastleggen van richtlijnen voor toegang tot de Computerruimtes om ongeautoriseerde toegang en- of ongeoorloofd handelen te voorkomen. Tevens zorgt deze procedure ervoor dat in de goederenstromen van en naar deze ruimtes beheerd worden waardoor gecontroleerde wijzigingen op de datacenters plaats vinden en de CMDB administratie actueel blijft. Deze procedure geldt voor iedereen die toegang krijgt tot de Computerruimtes.

1.2 Rollen

<i>Rol</i>	<i>Omschrijving</i>
Computerruimte-beheerder	IDC-A is eigenaar van de Computerruimtes en daarmee verantwoordelijk voor toezicht op alle activiteiten die op de Computerruimtes gebeuren. IDC draagt zorg voor: - Aanvraag procedure passen/autorisatie; - Uitgifte/Inname procedure passen/autorisatie; - Technische beveiligingsmiddelen zoals intercom, videobewaking, paslezers en of sloten; - Registratie, afhandeling informatiebeveiligingsincidenten; - Registratie aanmeldingen via paslezer; - Opstellen, actualiseren toegangsprocedure; - Periodieke controle op naleving; Een aantal van de uitvoerende beheer taken heeft IDC gedelegeerd aan HAAGnet.
HAAGnet	Draagt zorg voor het dagelijkse beheer van de Computerruimtes Om dit te realiseren voeren zij de volgende taken uit: Helpdesk - het registreren en beoordelen en van alle toegangsaanvragen. Toegangverlenen in overleg met Security Management van het IDC/A - (telefoonische) beschikbaarheid tijdens kantoor tijd van 7.30 tot 17.30 voor het verwerken van toegang aanvragen - Controle op toegang tot de ruimtes - rapportage van incidenten / onvolkomenheden m.b.t. ruimtes aan IDC Beheer

	- registratie van (security) incidenten / onvolkomenheden m.b.t. ruimtes - de begeleiding van onbevoegde interne en externe partijen binnen en buiten kantoor tijd. - Registratie van geïnstalleerde of afgevoerde apparatuur / programmatuur - controle op de uitgevoerde werkzaamheden (ook van de VOS groep): - verwerken in bijlage 2 weergegeven toegangsbon - controle op de werking van de door de change geraakte functionaliteit
IDC/A	Door security geautoriseerde medewerkers van IDC Server beheer krijgen op basis van individuele pas autorisatie, direct toegang tot de computer ruimtes. De toegang wordt verleend om de benodigde serverbeheer werkzaamheden uit te kunnen voeren. Mbt ruimte beheer hebben zij de volgende taken: - melden van (security) incidenten / onvolkomenheden m.b.t. ruimtes aan de HAAGnethelpdesk en aan de security manager IDC-A - de begeleiding van onbevoegde interne en externe partijen tbv serverbeheer werkzaamheden binnen kantoor tijd en de verantwoordelijkheid voor de door deze partijen verrichte handelingen - Melden aan HAAGnethelpdesk indien onbevoegde derde de computerruimtes gaan betreden - Registratie van geïnstalleerde of afgevoerde server apparatuur / en HAAGnet hierover informeren vlg formulier zie bijlage 2 - controle op de werking van de door de change geraakte functionaliteit - Bij het verwijderen van apparatuur direct opdracht verstrekken voor het verwijderen van patchkabels en sluiten van poorten aan HAAGnet
IDC/Technisch Beheer	Draagt zorg voor monitoring en onderhoud van de omgevingscondities van de Computerruimtes. Door security geautoriseerde medewerkers van IDC technisch beheer krijgen op basis van individuele pas autorisatie, direct toegang tot de computer ruimtes. De toegang wordt verleend om de benodigde technisch beheer werkzaamheden uit te kunnen voeren. Mbt ruimte beheer hebben zij de volgende taken: - melden van (security) incidenten / onvolkomenheden m.b.t. ruimtes aan de HAAGnethelpdesk en aan de security Manager - de begeleiding van onbevoegde interne en externe partijen tbv ruimtebeheer werkzaamheden binnen kantoor tijd en de verantwoordelijkheid voor de door deze partijen verrichte handelingen - Minimaal 24 uur van te voren melden aan HAAGnethelpdesk indien onbevoegde derde de computerruimtes gaan betreden - Registratie van geïnstalleerde of afgevoerde ruimtebeheerapparatuur / en HAAGnet hierover informeren vlg formulier zie bijlage 2 - controle op de werking van de door de change geraakte functionaliteit - Bij het verwijderen van apparatuur direct opdracht verstrekken voor het verwijderen van patchkabels en sluiten van poorten aan HAAGnet

IDC/A Security Manager	De security manager is verantwoordelijk voor de veiligheid van de computerruimtes en heeft hiervoor de volgende verantwoordelijkheden: Draagt zorg voor het opstellen en implementeren van de toegangsprocedure. Draagt zorg voor regelmatige controle van naleving van deze procedure en gedane registraties. Behandelt aanvragen voor toegang tot de ruimtes en bepaalt wie hiervoor geautoriseerd worden. Beheert de lijst met personen die toegang hebben tot de computerruimtes. Informeert IDC beveiliging en de HAAGnet helpdesk indien de lijst wordt aangepast Stuurt IDC beveiliging aan om op basis van de pas autorisatie aan te passen Kan uitdraaien van de pasjeslezers van de Computerruimtes opvragen. Draagt zorg voor de afhandeling van beveiligingsincidenten die zich in de Computerruimtes voordoen. Is geautoriseerd tot het opvragen van beeldmateriaal bij IDC beveiliging en toezicht. De geautoriseerde medewerker informeren over de in paragraaf 8 weergegeven richtlijnen Is geautoriseerd voor het ontzeggen en intrekken van een autorisatie op de persoonlijke pas bij niet opvolgen richtlijnen ?
IDC/Beveiliging, receptie en toezicht	Draagt zorg voor het beheer en wijzigen van autorisatie van de passen voor de Computerruimtes in opdracht van de IDC/A security manager. Draagt zorg voor de camerabewaking en toegangsdeurenbeveiliging op basis van de door de security manager aangeleverde toegangslijsten. Kan op verzoek een uitdraai van de pasjeslezers en de camerabeelden van de Computerruimtes verschaffen aan de IDC/A security manager. Wisselpassen vervallen.
BHV	BHV'ers hebben toegang tot de computerruimtes om bij ongevallen of noodsituatie op deze lokaties ondersteuning te kunnen geven. Door security geautoriseerde BHV'ers krijgen op basis van individuele pas autorisatie, direct toegang tot de computer ruimtes Zij betreden de computerruimtes alleen bij ongevallen of noodsituaties
Directeur IDC	Beoordeelt en autoriseert de aanvragen voor een uitdraai van de pasjeslezers van de Computerruimtes en de camerabeelden.

2 Autorisatieprocedure

De autorisatie voor toegang tot de Computerruimtes is alleen mogelijk met daarvoor toegekende autorisaties op persoonlijke pas. Deze pas dient te zijn voorzien van een pasfoto zodat voor het betreden van de ruimte de ware identiteit kan worden vastgesteld door de centrale meldkamer.

De aanvraag voor autorisatie moet bij de security manager per mail worden ingediend door de leidinggevende van de desbetreffende persoon.

Bij de aanvraag moet minimaal worden vermeld:

Voor en achternaam desbetreffende medewerker

Pasnummer

Afdeling

Reden voor autorisatie.

De security manager bepaalt of de aanvraag akkoord is en bij akkoord geeft hij de IDC beveiliging opdracht om de pasautorisatie aan te passen. Na aanpassing informeert IDC beveiliging de Security Manager de aanpassing heeft plaats gevonden.

De Security Manager past de toegangslijst aan en informeert de aanvrager en de HAAGnet helpdesk.

De Security Manager informeert per kwartaal de leidinggevende die toegang aangevraagd hebben over de mensen die onder hun naam toegang hebben. De leidinggevende is zelf verantwoordelijk om de door hem aangevraagde autorisatie op te heffen door hiervoor een mail aan de Security Manager te sturen.

2.1 Autorisatie passen

Het IDC/Serviceplein draagt zorg voor de daadwerkelijke pasautorisatie.

.

3. Procedure verzoek om toegang

3.1 Algemeen

Voor de naleving van de procedure is onderscheid gemaakt tussen verschillende vormen van werkzaamheden, te noemen:

- Geplande werkzaamheden tbv Serverbeheer, technisch-beheer of HAAGnet;
Hiervoor dient minimaal 24 uur vooraf per mail melding van gemaakt te worden bij de HAAGnet helpdesk.
In deze melding wordt aangegeven:

Verwachte aanvangstijd

Verwachte eindtijd

De geautoriseerde persoon die voor begeleiding van deze werkzaamheden zorgt

Voor en achternaam van de persoon (Personen) die de werkzaamheden gaat uitvoeren

Bedrijfsnaam

Legitimatie of Gemeente Pasnummer

Aard van de werkzaamheden

Risico's die deze werkzaamheden zou kunnen opleveren

De HAAGnet helpdesk controleert en bepaalt of er extra voorzorgsmaatregelen getroffen dienen te worden.

HAAGnet helpdesk geeft per mail akkoord voor de werkzaamheden.

De werkzaamheden aan ICT componenten dienen op basis van het reguliere changeproces te worden afgehandeld en dus met goedkeuring van changemanagement.

De HAAGnet Helpdesk registreert ook de aanvragen voor toegang buiten kantoortijd. De desbetreffende beheerafdeling zorgt voor begeleiding indien derde partijen tbv hun beheerdomein werkzaamheden op de computerzalen buiten werktijd moeten uitvoeren.

- Storingen; het verhelpen van een storing. Indien direct toegang benodigd is voor storingen geldt de noodprocedure. (Zie hoofdstuk 6, noodprocedure)
- Dagelijks beheer en Service Windows; het dagelijkse beheer van de servers op de Computerruimtes wordt gedaan door de geautoriseerde groep medewerkers van de gemeente Den Haag. Voor de werkzaamheden door de beheergroep worden uitgevoerd dient dit vooraf per mail bij de HAAGnet helpdesk te worden aangegeven.

3.1.1 Werkzaamheden in de kast van een andere partij

Toegang tot een kast van een andere partij is niet mogelijk. Dienen er toch door derden of andere beheerders werkzaamheden verricht te worden in of bij een kast van een andere partij, dan vinden de werkzaamheden onder regie van de kastbeheerder plaats.

Is dit niet het geval, dan zal de toegang tot de systemen van de betreffende partij geweigerd worden. De medewerker van de HAAGnet Helpdesk stemt dit met gemandateerde van de betreffende partij af en registreert de goedkeuring in de betreffende melding.

3.2 Registratie van legitimatiebewijs

Alle partijen die een bezoek willen brengen aan de Computerruimtes, moeten er rekening mee houden dat er om legitimatie gevraagd zal worden door de medewerker van de HAAGnet Helpdesk. Wanneer deze niet overhandigd kan worden, wordt de toegang geweigerd. Pasjes van een bedrijf van een derde partij worden niet als legitimatie gezien. Derde partijen dienen zich te laten registreren op basis van een officieel erkend legitimatiebewijs.

Bij twijfel neemt de HAAGnet Helpdesk contact op met de security Manager. Deze heeft het recht om een ieder de toegang te ontfagen of van de vloer te verwijderen bij twijfel en/of op redelijke gronden.

3.3 Beschrijving procedure verzoek om toegang

De onderstaande procedure heeft betrekking op iedereen die toegang wil tot de Computerruimtes.

Toegang tot de computerruimtes kan alleen verleend worden onder toezicht/ verantwoordelijkheid van een geautoriseerde beheerder. Deze beheerder is verantwoordelijk voor de gevolgen van de handelingen die onder zijn regie worden verricht.

Toegang dient vooraf per mail bij de HAAGnet helpdesk te worden aangekondigd waarbij HAAGnet voor een centraletoegangsregistratie zorgt.

1

Iedere geautoriseerde medewerker dient op de hoogte te zijn van de (gedrags-)richtlijnen voor het werken in computerruimtes zoals beschreven in hoofdstuk 8 van dit document.

De geautoriseerde beheerder dus de in de aanvraag genoemde begeleider draagt zorg voor controle van gedane werkzaamheden en ondertekening van het toegangsformulier (bijlage 2)

Indien de werkzaamheden zijn gestart tussen 07:00-19:00 uur maar dreigen uit te lopen buiten het window dient de HAAGnet Helpdesk hiervan op de hoogte te worden gebracht zodat hiervan melding gedaan kan worden bij IDC/BRT. (Zie hoofdstuk 4, toegang buiten kantoortijd). De opgegeven geautoriseerde beheerder blijft verantwoordelijk voor afhandeling en het tekenen van het toegangsdocument

4 Toegang buiten kantoortijd

Voor toegang na 19:00 tot 07:00 uur op werkdagen en in het hele weekend is de procedure toegang buiten kantoortijden van toepassing. De procedure voor toegang na 19:00 tot 07:00 uur voor derde partij is hetzelfde als beschreven in Hoofdstuk 3. Door de HAAGnet Helpdesk wordt dan bij de CMK toegang tot de panden aangevraagd.

Alleen de HAAGnet Helpdesk en de escalatiecontactpersonen (zie hoofdstuk 9) kunnen bij de CMK toegang buiten het window aanvragen.

4.1 Procedure

Minimaal 8 uur voor aanvang van de werkzaamheden dient door de HAAGnet Helpdesk per mail toegang te worden aangevraagd aan de CMK. In de mail dient minimaal het volgende te worden aangegeven.

- Meldingnummer HAAGnet Helpdesk
 - de datum en begin en eindtijd waarbinnen toegang benodigd is,
 - de naam van de persoon plus firmanaam van degenen voor de toegang benodigd is,
 - naam pas nr geautoriseerde beheerder
- (Bij verstoring van de emailomgeving volstaat een telefoontje)

De Centrale Meldkamer houdt van deze meldingen ook logging bij.

CMK verzorgt indien noodzakelijk ook de toegang tot de panden waar de computerruimtes zich bevinden.

Indien de werkzaamheden ook buiten het openingswindow worden afgerond dient de CMK ook weer te worden ingeschakeld om de persoon naar buiten te begeleiden en om het pand weer op slot te doen. Hiertoe dient dan de persoon die werkzaamheden aan het verrichten is weer contact op te nemen met de Meldkamer, die dan de deur van de Computerruimtes kan openen

Standaardafpraak met de CMK is dat men na een oproep binnen 30 minuten op locatie aanwezig is.

Mocht er in dit proces buiten het window wat mis gaan dan is de Centrale Meldkamer het eerste aanspreekpunt. (Zie voor contactgegevens hoofdstuk 9)

5 Procedure opvragen toegangslijsten en camerabeelden

De pasjeslezers registreren alle verzoeken tot toegang. De camera's registreren alle bewegingen. Deze gegevens worden 72 uur bewaard.

Op verzoek en met goede reden kan bij IDC/BRT om een uitdraai of opvraag van de vastlegging van deze gegevens worden gevraagd. Dit kan voor de Computerruimtes alleen door de Security Manager.

Dit verzoek wordt dan door IDC/BRT ter autorisatie voorgelegd aan de Directeur IDC. Na akkoord kunnen de gegevens aan de Security Manager worden uitgereikt. Deze handelt het verzoek verder af.

5.1 Rapportage

De Centrale Meldkamer levert haar registratie van de toegang wekelijks aan bij de HAAGnet Helpdesk. (maandag voor 12:00 uur, van de registraties van de afgelopen week).

HAAGnet controleert of de registratie overeenkomt met de geregiteerde aanvragen.

Bij afwijking wordt de securityManager hierover voor de eerst volgende woensdag geïnformeerd

HAAGnet Helpdesk levert de totale registratie van de toegangs aanvragen aan het IDC/A in de HAAGnet maandrapportage.

Op verzoek kan bij de HAAGnet Helpdesk om een uitdraai/opvraag van de vastlegging van deze gegevens worden gevraagd via de Security Manager.

6 Noodprocedure

In geval van calamiteiten is het niet mogelijk om 24 uur van tevoren toegang aan te vragen. Hiervoor geldt dan de noodprocedure. Indien met spoed toegang nodig is tot de Computerruimtes kan dit altijd na toestemming van een van de escalatiecontactpersonen. Zij zijn dan verantwoordelijk en dragen ervoor zorg dat de medewerkers van de gemeente Den Haag en eventuele leveranciers naar binnen worden gelaten, de begeleiding verzorgd wordt volgens de opgestelde procedure.

Indien in geval van storingen toegang tot de Computerruimtes buiten het openingswindow noodzakelijk is, kunnen de escalatiecontactpersonen direct contact opnemen met de Centrale Meldkamer. Om zeker te weten dat het deze escalatiecontactpersonen betreft wordt altijd door de Centrale Meldkamer teruggebeld op de daar bekende telefoonnummers. (Voor contactgegevens zie Hoofdstuk 9).

De Centrale Meldkamer zorgt dat het pand wordt geopend en zelfs in sommige gevallen dat de mensen op afstand worden toegelaten tot de Computerruimtes.

Mocht er in dit proces buiten het window wat mis gaan dan is de Centrale Meldkamer het eerste aanspreekpunt. (Zie voor contactgegevens hoofdstuk 9)

Na afloop van de storing dient er door de Escalatiecontactpersoon dan altijd per mail wel een kort verslag van verloop van de spoedwerkzaamheden te worden gedaan aan de HAAGnet Helpdesk en Security Manager. (zie voor contactgegevens hoofdstuk 9)

7 Beveiligingsincidenten

De definitie van een informatiebeveiligingsincident is:

Een onwenselijke of onverwachte gebeurtenis met een hoge kans tot het ernstig verstoren van de gemeentelijke operatie waarbij tevens dreiging ontstaat voor de beveiliging van informatie met mogelijk impact op de gemeentelijke administratie, gegevens van burgers of de reputatie van de Gemeente.

Voorbeelden zijn:

Menselijke fouten

Ongeautoriseerde fysieke toegang

Ongecontroleerde wijzigingen op systemen

Naleving van deze procedure en aanverwante gedragsregels is van groot belang voor de beveiliging van informatie van de Gemeente Den Haag.

Eventuele opgemerkte incidenten met betrekking tot het niet naleven van deze procedure of het niet of niet goed functioneren van de technische infrastructuur met betrekking tot de toegangsverlening dienen zo snel als mogelijk te worden gemeld aan de Security Manager (zie voor contactgegevens hoofdstuk 9)

Deze is verantwoordelijk voor het registreren, bewaken en aansturen van het oplossen van deze beveiligingsincidenten.

Interne medewerkers en derde partijen dienen zich te houden aan wat in deze procedure beschreven staat. Indien betrokkenen opzettelijk handelen in strijd met deze voorschriften, dan dienen disciplinaire maatregelen te worden genomen zoals

Opheffen pasautorisatie toegang datacentra,

Ontzegging toegang tot datacenters

Ontzegging toegang pand

8 Richtlijnen

8.1 Gedragsregels voor het werken in computerruimtes

- Het is niet toegestaan om licht ontvlambare, explosieve, giftige of radioactieve stoffen, zuren of basen, of containers met gas onder druk binnen op de Computerruimtes te brengen.
- Het is niet toegestaan de Computerruimte te betreden onder invloed van alcohol of andere roesverwekkende of bedwelmende middelen die mogelijk invloed kunnen hebben op motoriek en/of geestesgesteldheid van personen.
- In de Computerruimtes gelden algemeen geldende fatsoensnormen.
- Om de (klant-)apparatuur te bereiken dient men de kortste weg te gebruiken.
- Het is niet toegestaan om vloeistoffen in de Computerruimtes mee te nemen.
- Het is niet toegestaan om in de Computerruimtes te roken of open vuur te gebruiken.
- Het is in de Computerruimtes niet toegestaan eet- en drinkwaren mee te brengen en/of te nuttigen.
- Toegangsdeuren tot de Computerruimtes dienen, uitgezonderd bij toegang, altijd gesloten te zijn.
- Bij betreden van de ruimte wordt gebruik gemaakt van videoregistratie.
- Indien men beeld- en/of geluidopnamen op de computervloer maakt, is vooraf toestemming van de Security Manager IDC/A verplicht.
- Het is niet toegestaan apparatuur te bedienen of te verplaatsen waarvan men niet de eigenaar of huurder is.
- Het is niet toegestaan, direct of indirect, kabels aan te raken of te verplaatsen waarvan men niet de eigenaar of huurder is.
- Het is niet toegestaan fysieke wijzigingen aan te brengen in de Computerruimtes door bijvoorbeeld het verplaatsen van vloertegels.
- Bij alarm dient men de computervloer zo spoedig mogelijk te verlaten.
- Het is niet toegestaan verspanende werkzaamheden (zoals boren, knippen, strippen en slijpen) in de Computerruimtes te verrichten. Eventueel stof ontstaan door overige werkzaamheden dient direct verwijderd te worden m.b.v. een stofzuiger die te verkrijgen is bij de HAAGnet Helpdesk. Dit geldt ook voor einden van zgn. tie-wraps, afval van gestripte bedrading, etc.
- Het is uitsluitend toegestaan (klant-)apparatuur te plaatsen in de door HAAGnet Helpdesk toegewezen apparatuurkast(en) en werkzaamheden te verrichten aan eigen (klant-)apparatuur.
- Het is uitsluitend toegestaan gebruik maken van de toegewezen elektriciteitsvoorziening. In geval van storingen aan deze voorziening dient dit direct bij HAAGnet Helpdesk te worden gemeld. Voedingen, van welke aard dan ook (48V en/of 230/380V) die niet in de gehuurde kast staan, mogen niet zonder toestemming van HAAGnet Helpdesk worden uit- of ingeschakeld.
- Solderen, lassen, slijpen en alle vergelijkbare werkzaamheden die warmte veroorzaken zijn niet toegestaan. Kosten van een onnodige blussing en/of vervolgschade worden verhaald op de verantwoordelijke interne dienst.
- Renovatie van de Computerruimtes gebeurt alleen in opdracht of na goedkeuring van Hoofd SO /IDC/A.
- Bijzonderheden dienen direct te worden gemeld aan de HAAGnet Helpdesk
- Bij installatie, onderhoud en bediening van de (klant-)apparatuur dienen te allen tijde de installatie- en veiligheidsinstructies van de fabrikant te worden opgevolgd.

- Verpakkingsmaterialen van apparatuur dienen uit de Computerruimtes te worden verwijderd. Alle ruimtes dienen schoon en in ordentelijke staat achtergelaten te worden. Eventueel ontstane rommel in de Computerruimtes dient direct verwijderd te worden.
- Het gebruik van mobiele telefoons in de Computerruimtes is toegestaan. Dit betekent dat de te plaatsen apparatuur tegen instraling van GSM/apparatuur bestand dient te zijn.
- Na afloop dienen de werkzaamheden te worden afgemeld bij de HAAGnet Helpdesk.
- Bij vertrek dient het licht uit te worden gedaan en de Computerruimtes te worden afgesloten.

9 Functie- & Contactpersonenlijst

HAAGnet Helpdesk

Rol	Functie	Naam	Contactgegevens
Algemeen Contact 24x7	Helpdesk	HAAGnet Helpdesk	070-3538060 Mail: HAAGnet@KPN.com
Escalatiecontact 24x7	Site Manager	Loek Jonk	070-3538062 Mail: Loek.Jonk@KPN.com

IDC/A

Rol	Functie	Naam	Contactgegevens
Escalatiecontact 24x7	Infrabeheer Manager van dienst	Peter Groot, de Zie Rooster	070-3533002 06-52407654 peter.degroot@denhaag.nl Zie Rooster
Escalatiecontact 24x7	Security Manager	Peter van Eijk	070-3535460 06-52098266 Peter.vaneijk@denhaag.nl

IDC/Beveiliging receptie en toezicht

Rol	Functie	Naam	Contactgegevens
Coördinatie toegang	Meldkamer	Meldkamer (24x7)	070-3532400 centrale meldkamer@denhaag.nl
Escalatiecontact	Hoofd IDC/ BRT	Eldert Bakker (Tijdens kantooruren) Martijn Sonderwal (Tijdens kantooruren) (buitenkantooruren) Wachtdienst	070-3532426 06-21592750 Eldert.bakker@denhaag.nl 070-3538046 06-51415229 Martijn.sonderwal@denhaag.nl Via Meldkamer 070-3532400

IDC/Technisch Beheer

Rol	Functie	Naam	Contactgegevens
Algemeen Contact	Toegang	Serviceplein	070-3532455 serviceplein@denhaag.nl
Escalatiecontact	Hoofd IDC/ Technische Beheer	Ronald Poots	070-3532439 ronald.poots@denhaag.nl

Bijlage 1:

Overzicht Computerruimtes IDC/A

Locatie	Ruimte/kamernummer	Functie	Partijen
Leyweg		Datacenter	IDC/A, HAAGnet.
Spui	KMER	MER	IDC/A, HAAGnet
	TMER	MER	IDC/A, HAAGnet, ASR
	GMER	MER	IDC/A, HAAGnet

Bijlage 2:

Opleverdocument werkzaamheden Datacentra Gemeente Den Haag							
Opdrachtgever Gemeente Den Haag							
Naam Uitvoerende partij (bedrijf)afdeling							
Naam uitvoerende							
Telnr. uitvoerende							
Uit te voeren werkzaamheden							
Datum tijd aanvang werkzaamheden :							
Datum tijd oplevering werkzaamheden							
Geïnstalleerde of verwijderde apparatuur:							
Aantal							
	Merk						
	Type						
	Serie nr						
Locatie							
Adres							
Kamer							
	Kastruimte						
	Patch nr						
Geïnstalleerde of verwijderde connecties							
Aantal							
	Benaming						
	Reg nr						
Locatie							
Adres							
Kamer							
	Kastruimte						
Akkoord voor correctie oplevering							
Naam uitvoerende							
Datum							
Handtekening							
Verantwoordelijke beheerder							
Naam beheerder							
Datum							
Handtekening							