

Bedrijfscontinuïteitsplan - Het Gegevenshuis

Inhoud

1. Algemeen.....	2
1.1 Doel en doelgroep	2
1.2 Reikwijdte	2
1.3 Calamiteit	3
1.4 Kritische processen.....	4
1.5 Analooq en Digitaal archief	4
2. Organisatie Continuïteitsbeheer	6
2.1 Crisisteam	6
2.2 Overige betrokkenen en ketenpartners	9
2.3 Communicatie	9
3. Continuïteitsbeheer.....	10
3.1 Continuïteit bedrijfsprocessen	10
3.2 Afhankelijkheid van derden.....	10
4. Activering bedrijfscontinuïteitsplan	11
5. Testen Bedrijfscontinuïteitsplan.....	13
Bijlage 1 - Bereikbaarheidsgegevens.....	14

Bronvermelding

Bij het opstellen van dit document is gebruik gemaakt van de informatie over bedrijfscontinuïteitsmanagement van de Vereniging van Nederlandse Gemeenten/Informatiebeveiligingsdienst voor gemeenten”, licentie onder: CC BY-NC-SA 4.0

Wijzigingsoverzicht

Datum	Status/wijzigingen
2-6-2025	Geactualiseerde versie n.a.v. uitgevoerde test van BCP (eind 2024).
12-6-2025	Concept besproken met MT. Kritische processen HGH vastgesteld
18-6-2025	Concept gedeeld met contractmanagers
10-7-2025	Feedback contractmanagers verwerkt. Concept gedeeld met archivaris.
21-7-2025	Feedback archivaris (Toezicht HCL) verwerkt
3-9-2025	Vastgesteld door MT (versie 3.0)

1. Algemeen

Dit bedrijfscontinuïteitsplan omschrijft de acties die uitgevoerd dienen te worden nadat een calamiteit heeft plaatsgevonden die de voortgang van de kritische processen in gevaar brengt. Tevens zijn de taken en verantwoordelijkheden opgenomen.

De vorm en de omvang van het plan zijn bewust beperkt en beknopt uitgewerkt aangezien Het Gegevenshuis een kleine organisatie is met korte lijnen intern en naar het bestuur.

Dit plan is bedoeld voor intern gebruik bij het Gegevenshuis, voor het managementteam en de medewerkers om de procedure en het verloop van de communicatie bij een calamiteit inzichtelijk te maken. Bij inwerkingtreding van het calamiteitenplan wordt beoordeeld of deelnemers geïnformeerd moeten worden, afhankelijk van de impact op hun processen. Het plan is gepubliceerd in Scienta en voor alle medewerkers toegankelijk.

1.1 Doel en doelgroep

Het doel van dit plan is dan ook om de effecten van een calamiteit zoveel mogelijk te reduceren, de dienstverlening te continueren en het herstel te bespoedigen.

De doelgroep van dit continuïteitsplan zijn de functionarissen die bij uitval belast zijn met het zoveel mogelijk reduceren van de effecten van een calamiteit, het continueren van de bedrijfsprocessen van het Gegevenshuis en de voorbereiding op uitval.

1.2 Reikwijdte

De reikwijdte van dit bedrijfscontinuïteitsplan is gericht op de continuïteit van de kritische bedrijfsprocessen.

Voor calamiteiten in relatie tot bedrijfshulpverlening treedt het BHV ontruimingsplan in werking.

Buiten de reikwijdte van dit BCP vallen de uitbestede diensten aan de IT-leverancier en de faciliteiten die vallen onder de huurovereenkomst met de gemeente X (Faciliteren, onderhouden en beveiligen van het gebouw en de telefooncentrale). De contactgegevens van deze leveranciers zijn opgenomen in dit document.

1.3 Calamiteit

Een calamiteit wordt in het kader van dit continuïteitsplan gedefinieerd als een ongewenste gebeurtenis die zodanige negatieve gevolgen heeft dat de voortgang van de kritische bedrijfsprocessen van het Gegevenshuis wordt verstoord en de maximale uitvalsduur dreigt te worden overschreden. Mogelijke calamiteiten die kunnen leiden tot een ernstige verstoring van (kritische) bedrijfsprocessen zijn:

Calamiteit	Toelichting	Impact op kritische bedrijfsprocessen
Uitval gebouw	Bijvoorbeeld door: brand, uitval verwarming of koeling, bommelding, aanslag, defecte waterleiding, demonstraties etc.	Schade aan gebouw en apparatuur. Verlies van (analoge) informatie. Kantoorpand is niet toegankelijk. Processen kunnen op een andere locatie worden uitgevoerd
Uitval door stroomstoring	Storing bij energieleveranciers/ centrales.	Verstoring van IT-systemen en communicatie. Uitvoering van de processen is niet mogelijk
Uitval ICT	Bijvoorbeeld als gevolgen van problemen in de interne infrastructuur, computers, systemen, netwerk, software, communicatiemiddelen, etc.	Ernstige verstoring van (kritische) bedrijfsprocessen. Uitvoering van de processen is (deels) niet mogelijk.
Cybercrisis (cyberaanval)	Malware besmetting (virus, Ransomware, etc.) Als gevolg van cyberdreigingen en adviezen van NCSC en IBD uitschakelen van diensten	Continuïteit van de processen is verstoord. Data is versleuteld, niet beschikbaar, kans op verlies van data. Uitvoering van de processen is niet mogelijk. Kan leiden tot datalekken
Internet- of netwerkuitval (datacommunicatie)	Uitval mobiele en vaste telefonie. Uitval glasvezelverbinding. Storing bij (internet) provider.	Ernstige verstoring van (kritische) bedrijfsprocessen. Niet beschikbaar zijn van ICT-systemen.
Uitval Telefonie	Uitval mobiele en vaste telefonie.	Verstoring van communicatie met personeel en deelnemers. Processen kunnen worden uitgevoerd, maar kunnen hinder ondervinden.
Uitval Personeel	Epidemie, staking, ziekte etc.	Dienstverlening en halen van de wettelijke termijnen is verstoord

Bij calamiteiten wordt gebruik gemaakt van de [scenariokaarten](#) zoals deze beschikbaar worden gesteld door de informatiebeveiligingsdienst van de VNG. De belangrijkste contactgegevens worden toegevoegd in de bijlage van dit BCP.

1.4 Kritische processen

Voor het waarborgen van de continuïteit van de dienstverlening is het essentieel om inzicht te hebben in de processen die cruciaal zijn voor het functioneren van de organisatie. Deze zogenaamde kritische processen zijn de kernactiviteiten die, bij uitval of verstoring, direct leiden tot ernstige gevolgen voor de dienstverlening aan burgers, deelnemers en ketenpartners.

De meeste data zijn qua beschikbaarheid geclassificeerd op het niveau laag. Incidentele uitval van een week heeft hier geen onaanvaardbare gevolgen. De uitzonderingen zijn de processen waarbij een wettelijke verwerkingstermijn of een andere dringende reden een langere uitval niet toestaat. Deze kritische processen zijn opgenomen in de tabel hieronder.

Bedrijfsprocessen	Classificatie	Toelichting	Gewenste hervattijd
BAG-processen	Hoog	Wettelijke termijnen	24 uur
WKPB	Hoog	Wettelijke termijnen	24 uur
Huisaansluitingen (riooltelefoon)	Hoog	Verkeersveiligheid	24 uur
BGT	Midden	Wettelijke termijnen	48 uur

Daarnaast zijn een aantal processen en/of applicaties bedrijfskritisch voor de bedrijfsvoering van onze deelnemers, deze zijn in de tabel hieronder opgenomen.

Bedrijfsprocessen	Classificatie	Toelichting	Gewenste hervattijd
Beschikbaarstelling kaartviewer	Hoog	Borgen van de openbare orde en veiligheid bij calamiteiten en handhaven op straat	24 uur
Beschikbaarstelling applicatie beheer openbare ruimte	Hoog	Inzicht in openbare ruimte bij calamiteiten	24 uur

Uit beheersmatige overwegingen neemt Het Gegevenshuis voor alle niveaus dezelfde maatregelen, die voldoen aan de eisen voor het hoogste niveau. Deze eisen zijn vastgelegd in DVO en SLA met de IT-leverancier.

1.5 Analooog en Digitaal archief

Het Gegevenshuis is op grond van de Archiefwet verplicht om een calamiteitenplan voor de archiefruimte te hebben. Aangezien het Gegevenshuis grotendeels digitaal werkt en geen eigen archiefruimte heeft is, in overleg met de archivaris, ervoor gekozen dit plan op te nemen in het bedrijfscontinuïteitsplan. In dit hoofdstuk worden de verschillende “archieven” en de genomen maatregelen beschreven.

Digitaal archief

Digitale informatie is cruciaal voor de dienstverlening en interne bedrijfsvoering van Het Gegevenshuis. Het Gegevenshuis is eindverantwoordelijk voor de digitale archiefbescheiden, ook wanneer het beheer van de IT-omgeving is uitbesteed. In het kader van bedrijfscontinuïteit en de Archiefwet zijn maatregelen getroffen om bij calamiteiten zoals brand of ransomware de goede, geordende en toegankelijke staat van informatie te waarborgen. Dit omvat afspraken met de IT-leverancier over back-up, herstel, toegangsbeheer en monitoring, die periodiek worden getoetst.

Onderstaande tabel geeft een overzicht van de processen van Het Gegevenshuis die, conform de selectielijst 2020 de waardering te bewaren hebben, in geval van calamiteit dienen deze als eerste veilig gesteld te worden.

In het documentair structuurplan (neoforce) zijn deze processen verder uitgewerkt, inclusief de locatie van de bestanden.

Procesnaam	Bewaartermijn
Bestuurlijk overleg en besluitvorming	Bewaren
Opstellen meerjarenbegroting en jaarrekening	Bewaren
Visie en strategie Opstellen	Bewaren
Gemeenschappelijke Regeling instellen	Bewaren
(Informatie) beleid en procedures ontwikkelen	Bewaren
Vervanging, migratie en conversie uitvoeren	Bewaren
Metadateren en classificeren	Bewaren
Vernietigen van informatie	Bewaren
Huisnummerbesluiten (BAG)	Bewaren -Overdragen (mandaat)

Analoge archieven

Het Gegevenshuis heeft geen eigen archiefruimte en werkt grotendeels digitaal. Vanaf januari 2025 worden alle documenten uitsluitend digitaal ondertekent en wordt er geen nieuw analoog archief meer opgebouwd. Analoge archieven die wel nog bij HGH aanwezig zijn worden hieronder benoemd, inclusief de archieflocatie en de medewerkers met toegang.

Locatie	Archiefbestanden	Toegang
Kamer Managementassistente, Benedenverdieping naast trap. Afgesloten kast.	2015 – heden: • Personeelsdossiers • Contracten • Facturen	Directeur, Managementassistente Medewerker staf/Financiën

De analoge archieven zijn beperkt tot één afdelingskast en het betreft informatie die conform de Selectielijst 2020 voor vernietiging in aanmerking komt. Aangezien de dossiers ook grotendeels digitaal beschikbaar zijn, is een bewuste risicoafweging gemaakt. Het risico op verlies van deze documenten door waterschade, brand, plaagdieren/schimmel, elektriciteitsuitval, vandalisme of diefstal wordt geaccepteerd. Er worden daarom geen aanvullende beschermingsmaatregelen getroffen.

Losse gegevensdragers

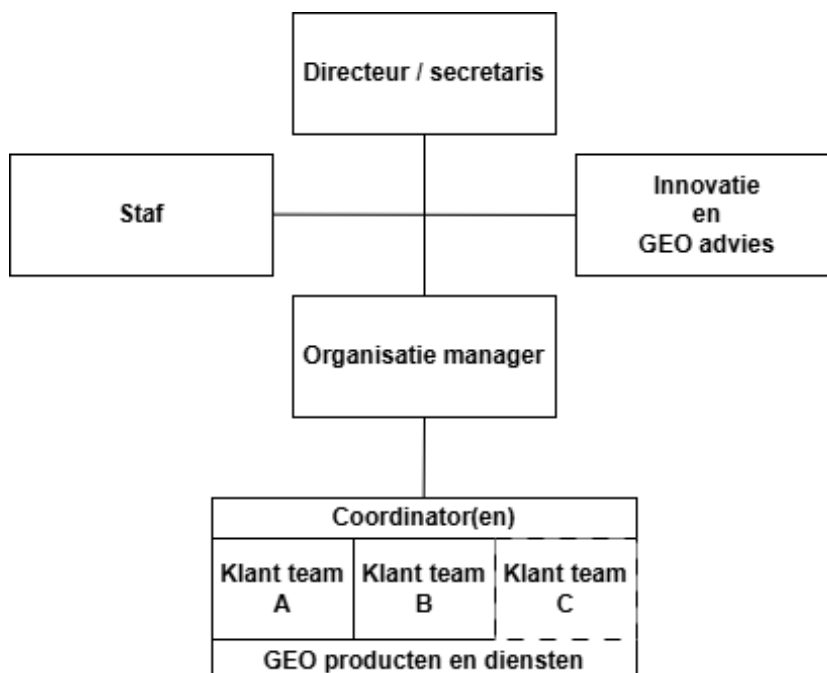
Naast analoge archieven bevinden zich bij HGH de harde schijven met beeldmateriaal van de deelnemers. Een beschrijving hiervan is opgenomen in de tabel hieronder.

Locatie	Archiefbestanden	Toegang
Kamer Datamanagement (2 ^e verdieping) in afgesloten kast.	2015 – heden: Beeldmateriaal (obliek-, luchtfoto's en panoramafoto's)	Medewerkers Datamanagement

Een deel van het beeldmateriaal is toegankelijk via kaartViewer, terwijl een ander deel uitsluitend is opgeslagen op losse harde schijven. Van het merendeel is een kopie beschikbaar. Er is een digitale inventarisatie opgesteld van deze gegevensdragers. Op korte termijn worden afspraken gemaakt met de deelnemende gemeenten over de overdracht van deze gegevens. Tot die tijd worden de kopieën op een alternatieve locatie opgeslagen. In het derde of vierde kwartaal van 2025 worden hierover nadere afspraken gemaakt met de IT-leverancier.

2. Organisatie Continuïteitsbeheer

In geval van een calamiteit wordt veelal gewerkt onder hoge druk. In een korte tijd dienen veel beslissingen te worden genomen, die grote gevolgen kunnen hebben. Op grond van deze kenmerken wordt tijdens een calamiteit vaak volgens een afwijkende organisatie dan in de normale situatie gewerkt. Ook in de crisissituatie geldt de hiërarchie die vastgelegd is in het organigram van Het Gegevenshuis.



2.1 Crisisteam

Het crisisbeheerteam vormt de kern van de crisisorganisatie van het Gegevenshuis en is verantwoordelijk voor de coördinatie en aansturing van alle activiteiten die nodig zijn om de continuïteit van kritische bedrijfsprocessen te waarborgen tijdens een calamiteit. Dit team treedt in werking zodra het continuïteitsplan wordt geactiveerd en opereert onder directe verantwoordelijkheid van het Dagelijks Bestuur van het Gegevenshuis (vertegenwoordigd door de Directeur).

De directeur heeft bij het crisisteam de rol van het centrale aanspreekpunt en coördineert de acties.

Het crisisbeheerteam heeft onder andere de volgende taken:

- Besluitvorming over maatregelen voor het waarborgen van kritische processen;

- Coördinatie van alle herstelactiviteiten binnen de organisatie;
- Toezicht houden op de voortgang en effectiviteit van de uitgevoerde maatregelen;
- Informeren van deelnemers, interne stakeholders en medewerkers;

Documenteren van alle acties ten behoeve van evaluatie en verbetering

Samenstelling

Behalve het Managementteam, bestaat het crisisbeheerteam uit functionarissen met expertise op het gebied van:

- ICT
- Facilitaire zaken
- Informatiebeveiliging en Privacy
- Bedrijfshulpverlening (BHV)
- Ondersteuning (verslaglegging, etc.)

De exacte samenstelling is afhankelijk van de situatie en de calamiteit.

Taken en verantwoordelijkheden

Dagelijks Bestuur

De voorzitter van de gemeenschappelijke regeling vertegenwoordigt primair Het Gegevenshuis in- en buiten rechte, dus ook bij calamiteiten. Externe communicatie met de media wordt ook gevoerd door de voorzitter van het Dagelijks Bestuur.

Directeur/- secretaris

Directeur/secretaris is door zijn mandaat verantwoordelijk voor de activering en het coördineren van het Bedrijfscontinuïteitsplan en stelt het crisisteam samen. Directeur/-secretaris nodigt interne en externe expertise uit om deel te nemen aan het crisisteam en organiseert het crisISOverleg afhankelijk van de situatie op locatie of online.

Besluitvorming op het gebied van de bedrijfsvoering is gemandateerd aan de Directeur/-secretaris. Hij legt de verantwoordelijkheid af aan het Dagelijks Bestuur. Dit geldt ook bij de besluitvorming bij een calamiteit. De directeur is verantwoordelijk voor de communicatie naar het bestuur en deelnemers (externe communicatie).

Organisatiemanager

De organisatiemanager is verantwoordelijk voor de coördinatie en het toezicht op de uitvoering van de taken die door het crisisteam worden bepaald. De organisatiemanager is ook verantwoordelijk voor de interne communicatie.

IT-Businessconsultant

De IT-Businessconsultant is verantwoordelijk voor het bewaken de continuïteitsafspraken met de IT-leverancier, het coördineren van herstelmaatregelen en het onderhouden van contact met de leverancier tijdens een calamiteit. Tevens is deze medewerker het aanspreekpunt en de coördinator bij de uitwijktest die jaarlijks door de IT-leverancier wordt uitgevoerd.

Adviseur privacy & informatiemanagement

Is verantwoordelijk voor het opstellen, actualiseren en testen van het Bedrijfscontinuïteitsplan Het Gegevenshuis.

Is verantwoordelijk voor het waarborgen van de informatiebeveiliging en privacy tijdens de crisis, inclusief het beoordelen van risico's en het adviseren over maatregelen om de integriteit, beschikbaarheid en vertrouwelijkheid van informatie te beschermen.

Bij een privacy- en informatiebeveiligingsincident (datalek, ransomware) is de privacy officer de contactpersoon voor Informatiebeveiligingsdienst (IBD), Autoriteit Persoonsgegevens. Indien Het Gegevenshuis verwerkingsverantwoordelijke is bij een datalek, zorgt de privacy officer voor de melding bij de Autorisatie persoonsgegevens (in overleg met de Functionaris Gegevensbescherming)

Medewerker facilitaire zaken

Verantwoordelijk voor het coördineren van de inzet van externe partijen voor gebouwbeheer en voorzieningen tijdens een calamiteit en het informeren van het crisisbeheerteam over de status van huisvesting en gebouwtoegang.

Hoofd Bedrijfshulpverlening

Bij een calamiteiten waarbij het pand ontruimd moet worden zorgt het Hoofd-BHV voor de ontruiming van het pand volgens Ontruimingsplan BHV en informeert het managementteam

Medewerkers Bedrijfsbureau

Bij de inwerkingtreding van het BCP wordt een logboek bijgehouden waarin alle genomen besluiten, acties, communicatie en bijzonderheden systematisch worden vastgelegd ten behoeve van evaluatie, verantwoording en eventuele bijstelling van het plan. Een van beide medewerkers van bedrijfsbureau is verantwoordelijk van het bijhouden van dit logboek (afhankelijk van soort crisis).

Crisislocatie

Primair: Emile Erensplein 55 te Landgraaf

Alternatief: Sweelingsplein 1, Landgraaf (opgenomen in DVO met gemeente Landgraaf)

Digitaal: via teams

Agenda crisisoverleg

Het crisisteam neemt bij het eerste overleg een besluit over de frequentie van de bijeenkomsten (vaste vergadercyclus, bijv. dagelijks om X.00 uur).

Tijdens het crisisoverleg wordt gewerkt met een vaste agenda volgens de BOB-methode (Beeldvorming, Oordeel, Besluit). Hierbij kan ter ondersteuning gebruik gemaakt worden van de [scenariokaarten](#) van de VNG.

1. Opening
Doel/status bijeenkomst, vergaderfrequentie, rol van de aanwezigen, juiste inhoudelijk deskundigen, lopende zaken stilleggen, vervanging, afspraken vergaderdiscipline, actiepunten, eindproducten en voortgang.
2. Beeldvorming
kort en feitelijk in kaart brengen van een situatie op basis van geverifieerde informatie, met aandacht voor relevante feiten, ontbrekende gegevens, betrokken partijen.
3. Oordeel
Welke kant kan deze crisis opgaan? Wat is realistisch, wat is het worstcasescenario, wat voor scenario verwachten we?
4. Besluit
Welke maatregelen kunnen worden genomen, bij voorkeur op basis van advies inhoudelijk deskundige.

5. Communicatie

Welke strategie, wat moet de boodschap zijn, zowel intern en extern?

6. Actiepunten vaststellen

Prioriteiten bepalen en acties uitzetten.

2.2 Overige betrokkenen en ketenpartners

Afhankelijk van de calamiteit wordt KWIS bij de gemeente Landgraaf (verhuurd pand en facilitaire zaken), de IT-leverancier (Solido), externe expertise, de deelnemers en de leveranciers betrokken.

Deze betrokkenen zijn op verschillende manieren van belang voor de hervatting van de kritische processen met waarborging van de eigen veiligheid. Ze brengen advies uit, voeren opgedragen activiteiten uit en doen mededelingen aan het crisisteam over de voortgang van de herstelactiviteiten.

2.3 Communicatie

Een goede communicatie heeft veel invloed op het succesvol uitvoeren van het bedrijfscontinuïteitsplan. De inwerkingstelling van het continuïteitsplan kan directe impact hebben op de continuïteit van de dienstverlening. De inwerkingstelling van het continuïteitsplan dient dan ook gecommuniceerd te worden aan alle doelgroepen en betrokkene.

Het Dagelijks Bestuur dient zo spoedig mogelijk, uiterlijk binnen één dag (24 uur) geïnformeerd te worden. Dit geldt ook voor de medewerkers en de contractmanagers.

Verantwoordelijkheden

Voorzitter Dagelijks Bestuur

De Gemeenschappelijke regeling Het Gegevenshuis wordt buiten rechte vertegenwoordigd door de voorzitter van Het Dagelijks Bestuur. De voorzitter communiceert met de media indien nodig bij een grote calamiteit.

Directeur/secretaris:

De Directeur/-secretaris krijgt formeel de toestemming van het Dagelijks Bestuur om de communicatie te coördineren binnen de organisatie bij een calamiteit. Hij is verantwoordelijk voor het communiceren met het Dagelijks Bestuur en de deelnemers.

De directeur is voorzitter van het crisisteam en onderhoudt het contact met het de organisatiemanager en het crisisbeheerteam.

De directeur voert ook de communicatie uit bij een ernstig letsel van een medewerker waarbij de familie ingelicht moet worden

Organisatiemanager

De organisatiemanager is verantwoordelijk voor de interne communicatie en is het aanspreekpunt van de medewerkers.

Communicatiemiddelen

Tijdens het crisisoverleg wordt bepaald welk communicatiemiddel wordt ingezet. Mogelijk opties zijn: intern: telefoon, Intranet, email, HGH-whatsappgroep, MS Teams
Extern: telefoon, email, internet, sociale media.

3. Continuïteitsbeheer

Om de continuïteit van kritieke bedrijfsprocessen te waarborgen, zijn maatregelen getroffen die de continuïteit zoveel als mogelijk te garanderen. Bij een calamiteit kunnen de processen verstoord worden. Daarnaast is in kaart gebracht welke processen afhankelijk zijn van derden.

3.1 Continuïteit bedrijfsprocessen

Uit beheersmatige overwegingen neemt het Gegevenshuis voor alle niveaus dezelfde maatregelen, die voldoen aan de eisen voor het hoogste niveau. Deze eisen zijn vastgelegd in het SLA met de IT-leverancier. De belangrijkste eisen zijn:

- Uitval is in principe niet toegestaan.
- Het informatiesysteem mag incidenteel voor maximaal twee dagen uitvallen.
- Het maximale verlies van data is één werkdag.
- De maximale hersteltijd in geval van incidenten is twee werkdagen.

Uitzondering hierop zijn de processen die een classificatie hoog hebben zoals beschreven in paragraaf 1.4, deze mogen maximaal 24 uur uitvallen (1 werkdag).

De proceseigenaren zijn verantwoordelijk voor het actueel houden van de bijbehorende procedures.

Doordat alle processen uitgevoerd worden in een virtuele omgeving is de beschikbaarheid van internet en de ICT-omgeving van de IT-leverancier cruciaal voor het uitvoeren van de processen. Als de uitval van internet of netwerk langer dan twee dagen duurt, kan Het Gegevenshuis niet meer voldoen aan de vastgelegde afspraken en afhandeltermijnen bij de kritische bedrijfsprocessen. In deze situatie worden de deelnemers geïnformeerd en een melding bij de Landelijke voorziening gedaan.

Als uitval uitsluitend geldt voor de locatie Emile Erensplijn 55 kunnen de medewerkers vanaf elke locatie de werkzaamheden continueren.

3.2 Afhankelijkheid van derden

Voor processen waarbij onze organisatie afhankelijk is van derden zijn afspraken gemaakt over maximale uitvalstermijnen en herstelmaatregelen.

Leverancier	Dienstverlening	Getroffen maatregelen
Gemeente Landgraaf	De in pandige bekabeling is gefaciliteerd en wordt onderhouden door de gemeente Landgraaf.	Onderhouds- en herstelwerkzaamheden zijn vastgelegd in de Dienstverleningsovereenkomst met de gemeente Landgraaf.
Gemeente Landgraaf	Telefooncentrale in beheer door de gemeente Landgraaf.	Alle medewerkers zijn naast het vaste nummer dat via centrale loopt ook bereikbaar via het mobiele nummer.
Gemeente Landgraaf	Inbraakpreventie	Het pand is beveiligd door anti inbraak alarmsysteem. De meldingen van de alarmcentrale Brinkman ontvangt de bode van de gemeente Landgraaf, deze is 24/7 ook in het weekend bereikbaar. Hiervoor bestaat een procedure bij gemeente Landgraaf.

Gemeente Landgraaf	Verhuur pand (facilitaire diensten, printers)	Afspraken vastgelegd in DVO.
Solido – IT-leverancier	ICT-diensten	Afspraken aangaande beschikbaarheid van het netwerk en systemen zijn vastgelegd in het contract en servicelevel agreement met de IT-leverancier. Deze neemt de maatregelen zoals back-up, systemen redundant uitvoeren, monitoring en logging van het netwerk intern en extern, uitvoeren van de uitwijktesten. Periodieke SLA en security overleggen, afstemming.
Solido – IT-leverancier	Faciliteren van apparatuur (laptops, mobiele telefoons, docking stations)	Contract en SLA aangaande Mobile Device management, monitoring IT-leverancier
IBD	Ondersteuning bij de calamiteiten	De IBD biedt ondersteuning in geval van een incident om schade te beperken en de situatie op te lossen. De CERT is 24x7 bereikbaar en kan bij ernstige of complexe incidenten de hulp inroepen van security experts, woordvoerders en/of het Nationaal Cyber Security Centrum (NCSC). Medewerker privacy en informatiebeveiliging is bij IBD geregistreerd als Vertrouwde Contactpersoon Informatiebeveiliging (VCIB) en ontvangt waarschuwingen en kwetsbaarheidsmeldingen die door IBD worden verstuurd om eventuele hack te voorkomen.
Zuidlease	Wagenpark	Leasecontract voor de reparatie, voor langdurige uitval samen met garage of intern kijken naar de alternatieven (vooral van belang bij de werkbussen van de landmeters).
LNR Globalcom (Alternatief Boels)	Vervanging landmeetapparatuur	In het onderhoudscontract van de leverancier LNR Globalcom is vastgesteld dat afhankelijk van de beschikbaarheid de apparatuur geleverd kan worden. Is tijdelijk leveren van de apparatuur via LNR Globalcom niet mogelijk dan wordt overwogen om deze te huren. Het blijft maatwerk afhankelijk van de situatie

4. Activering bedrijfscontinuïteitsplan

Na het ontstaan van een calamiteit treedt het continuïteitsplan in werking.

Dit moet zo snel mogelijk te gebeuren, zodat de noodzakelijke acties tijdig kunnen

worden gestart. Voor kritische bedrijfsprocessen met een hoge beschikbaarheid hoeft voor het inwerking stellen van het herstelscenario niet gewacht te worden op de activering van het gehele continuïteitsplan volgens de hierna beschreven procedures. Het Gegevenshuis heeft criteria opgesteld voor de activering van het Bedrijfscontinuïteitsplan.

Bij de activering van het BCP wordt afhankelijk van de calamiteit kunnen de scenariokaarten van de VNG als ondersteuning worden gebruikt. De scenariokaarten en het BCP zijn beschikbaar op de volgende locaties:

- In de team-omgeving van Datamanagement (HGH Datamanagement)
- Scienta
- Analooq op de kamers van bedrijfsbureau en Datamanagement en op de kamer bij de managementassistente.

Activering

Alarmering en opschaling van de crisisorganisatie vindt plaats volgens de vaste structuur en criteria die Het Gegevenshuis heeft opgesteld. In het geval van een serieus te nemen (dreigende) calamiteit, wordt het continuïteitsplan geactiveerd, met als doel om de bedrijfsprocessen te ondersteunen die nodig zijn om de doelstellingen van Het Gegevenshuis te behalen.

Criteria om BCP in werking te laten treden:

1. Ernstige verstoring van de beschikbaarheid van het netwerk en systemen waarbij de verwachting is dat het langer dan 24 uur gaat duren.
2. Cyberaanval. Versleuteling van data en systemen.
3. Stroomstoring op locatie. Als deze niet binnen 24 uur opgelost kan worden.
4. Brand, Bliksemschade, explosie, waterschade waardoor fysieke locatie niet beschikbaar is.
5. Inbraak, vernieling waardoor locatie niet toegankelijk is en apparatuur op locatie is vernield of gestolen waardoor continuïteit van de processen is verstoord.
6. Verlies en diefstal van grote aantallen apparatuur die niet binnen 24 uur vervangen kan worden en waardoor uitvoeren van de processen niet meer mogelijk is.
7. Groot aantal medewerkers is niet inzetbaar, hoog aantal ziekmeldingen door pandemie, waardoor dienstverlening en halen van de wettelijke termijnen in gevaar komt.

Stappenplan voor het inwerking treden van het BCP

1. Na het ontstaan van een calamiteit neemt de medewerker contact op met de organisatiemanager of de directeur.
2. Het managementteam onderzoekt situatie en maakt de afweging ten aanzien van aard, omvang en criteria
3. De directeur besluit om een crisioverleg te plannen.
4. Bijeenkomst Crisisteam: besluit nemen of bedrijfscontinuïteitsplan wordt geactiveerd (beeldvorming, oordeel, besluit)
5. Bij Activatie BCP worden alle in het plan opgenomen betrokkenen gewaarschuwd (afhankelijk van soort calamiteit)
6. Herstel en terugkeer naar normale werking
Tijdens herstelfase schaalde de crisisorganisatie af en worden de reguliere activiteiten hervat. Bij het hervatten van de activiteit worden de medewerkers ondersteund en wordt het hervatten gemonitord.
7. Nazorg en evaluatie
 - Analyseer wat goed en fout ging.

- Pas het BCP aan op basis van de lessen die zijn geleerd.
- Rapportage: Documenteer het volledige verloop van de crisis en de aanpak.

5. Testen Bedrijfscontinuïteitsplan

Het bedrijfscontinuïteitsplan wordt jaarlijks getest om de effectiviteit, toepasbaarheid en actualiteit van de beschreven maatregelen en procedures te waarborgen. Tijdens deze test wordt nagegaan of de organisatie in staat is om bij een verstoring of calamiteit de kritieke processen voort te zetten en de beschikbaarheid van essentiële informatie te garanderen. De test richt zich onder andere op:

- De werking van communicatieprotocollen;
- De toegankelijkheid van digitale informatie en back-ups;
- De samenwerking met de IT-leverancier bij herstelmaatregelen;
- De praktische uitvoerbaarheid van de beschreven procedures;
- De rolverdeling en verantwoordelijkheden binnen het crisisteam.

De test is verplicht en wordt gecoördineerd door de adviseur privacy & informatiemanagement, die verantwoordelijk is voor de voorbereiding, uitvoering en evaluatie. In overleg met de IT-leverancier wordt een realistisch scenario gekozen, gebaseerd op een van de in paragraaf 1.3 beschreven calamiteiten.

De resultaten van de test worden zorgvuldig gedocumenteerd. Eventuele knelpunten of verbeterpunten worden geanalyseerd en gebruikt om het bedrijfscontinuïteitsplan waar nodig aan te passen en te verbeteren.

Bijlage 1 - Bereikbaarheidsgegevens

In dit hoofdstuk zijn de bereikbaarheidsgegevens van alle intern en extern betrokkenen opgenomen.

Bereikbaarheidsgegevens interne betrokkenen

Functie	Naam	e-mailadres	Telefoonnr.
Directeur	Sjef Lenen	Sjef.leenen@gegevenshuis.nl	+31629087228
Organisatiemanager	Nicolle Prevo	Nicolle.prevo@gegevenshuis.nl	+31643751475
IT-Businessconsultant	Michel Vercruijse	Michel.vercruijse@gegevenshuis.nl	+31643751483
Facilitaire zaken	Yvonne van Lubeek	Yvonne.van.Lubeek@gegevenshuis.nl	+31655695652
Adviseur privacy & informatiemanagement (CISO)	Yvon Meertens	Yvon.meertens@gegevenshuis.nl	+31642343330
Hoofd BHV	Michel Vercruijse	Michel.vercruijse@gegevenshuis.nl	+31643751483
Staf – ondersteuning en bijhouden logboek	Robert Vluggen	Robert.vluggen@gegevenshuis.nl	+31614226818

Bereikbaarheidsgegevens extern betrokkenen

Dienst	Naam	e-mail	telefoonnummer
IT-leverancier	Solido	Incidentmanagement@solido-it.nl	045-5604912
Gebouw en facilitair	Gemeente Landgraaf, KWIS	kwis@landgraaf.nl	045-5695234
Verzekering	ZekerHeuts	Info@zekerheuts.nl	088-4504844
Toezicht en Advies Archiefwet	Historisch Centrum Limburg	toezichtenadvies@hclimburg.nl	043-3255500
Ondersteuning bij calamiteiten	IBD		070-2045511