ADDENDUM DIGITALE VEILIGHEID & PRIVACY
(DV&P ADDENDUM)

tussen

[NAAM WEDERPARTIJ]

en

Enexis Netbeheer B.V.

d.d. [datum]

Paraaf Enexis

Paraaf Wederpartij

INHOUDSOPGAVE

ONDERGETEKENDEN:

1) [Enexis Netbeheer B.V.] een besloten vennootschap met beperkte aansprakelijkheid statutair gevestigd te 's-Hertogenbosch, kantoorhoudende te 5223 MB 's-Hertogenbosch aan de Magistratenlaan 116, ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer 17131139, te dezen rechtsgeldig vertegenwoordigd door [naam] [functie] en [naam] [functie] hierna te noemen: Enexis

en

1) Wederpartij [naam en rechtsvorm] statutair gevestigd te <statutaire vestigingsplaats> kantoorhoudende aan <adres>, ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer [kvk-nummer] te dezen rechtsgeldig vertegenwoordigd door <naam> <functie> hierna te noemen: Wederpartij;

Ieder afzonderlijk aangeduid als "**Partij**" of gezamenlijk als "**Partijen**";

Overwegende dat:

- Partijen de overeenkomst [naam overeenkomst] met ingangsdatum [datum] hebben gesloten (hierna: de **Hoofdovereenkomst**), en dat op de Hoofdovereenkomst de Enexis Inkoopvoorwaarden 2025 (hierna: **AV**) van toepassing zijn verklaard. De Hoofdovereenkomst heeft betrekking op [omschrijving goederen, diensten en werkzaamheden];
- Enexis wegens haar rol in de vitale infrastructuur van Nederland als essentiële entiteit in de zin van de Cyberbeveiligingswet (**Cbw**) en kritieke entiteit in de zin van de Wet weerbaarheid kritieke entiteiten (**Wwke**) geldt en als zodanig gebonden is aan strikte wet- en regelgeving op het gebied van beveiliging en continuïteit;
- de vitale aard van de openbare taken van Enexis op het gebied van transport van elektriciteit, gas en warmte betekent dat uitval, verstoring of het compromitteren van systemen ernstige gevolgen kan hebben voor de leefbaarheid en bedrijfsvoering in grote delen van Nederland;
- Enexis de verantwoordelijkheid draagt om passende beveiligingsmaatregelen te implementeren met Wederpartij en te onderhouden;
- Enexis voortdurend de behoefte heeft aan het evalueren en verbeteren van beveiligingsmaatregelen tussen Partijen om te anticiperen en reageren op opkomende bedreigingen en risico's;
- Enexis een Digitale Veiligheid & Privacy Impact-analyse (**DV&P-analyse**) heeft uitgevoerd met betrekking tot de goederen, diensten en/of werkzaamheden onder de Hoofdovereenkomst, waarbij het risico als 'hoog' is vastgesteld;
- Partijen in dit DV&P Addendum in aanvulling op de Hoofdovereenkomst afspraken over de te implementeren en onderhouden beveiligingsmaatregelen vastleggen.

Zijn het volgende overeengekomen:

DEFINITIES

Wanneer in dit DV&P Addendum de termen worden gebruikt die zijn gedefinieerd in de AV, hebben die termen dezelfde betekenis als in de AV. Partijen hanteren in dit DV&P Addendum verder de onderstaande definities:

Definitie	Omschrijving
Beveiligingsmaatregelen	het geheel van beleid, processen, procedures en technische maatregelen die de beschikbaarheid, integriteit, kwaliteit en vertrouwelijkheid van alle vormen van Informatie, processen, goederen en/of diensten van Enexis en Wederpartij borgt en de eventuele gevolgen van Incidenten en/of Inbreuken beperkt en herstelt.
Derde(n)	een door Wederpartij bij de uitvoering van (een onderdeel van) de Hoofdovereenkomst ingeschakelde derde, waaronder begrepen onderaannemers en nevenaannemers. Van een Derde(n) is ook sprake bij het gebruik van goederen en/of diensten van derden door Wederpartij ten behoeve van Enexis.
DV&P-analyse	een interne Enexis analyse die, onder meer op grond van de aard, de continuïteitsrisico's en de mate van toegang tot Enexis Informatie en locaties door (medewerkers van) Wederpartij, de mate van het beveiligingsrisico voor Enexis aanduidt als 'midden' of 'hoog'.
Incident	in afwijking van artikel 32.17 AV, wordt onder Incident verstaan een inbreuk op de beveiliging waardoor de beschikbaarheid, integriteit of vertrouwelijkheid van Informatie bedreigd wordt of (gedeeltelijk) gecompromitteerd is dan wel een gebeurtenis die ertoe leidt dat continuïteit c.q. kwaliteit van de processen, goederen en/of diensten van Wederpartij en/of van Enexis (nadelig) beïnvloed kan worden, waaronder begrepen een Inbreuk.
Informatie	data, gegevens (waaronder Persoonsgegevens), databanken en informatie (waaronder Vertrouwelijke Informatie) betreffende de Enexis bedrijfsvoering in de breedste zin. Hieronder wordt begrepen alle door of namens Enexis te verstrekken/verstrekte informatie, hetzij mondeling, schriftelijk of in enige andere vorm, hetzij voorafgaand of gedurende de Hoofdovereenkomst, alsmede alle documenten en overige gegevens in welke vorm dan ook die informatie bevat of weergeeft of die voortkomt uit de informatie die aan Wederpartij wordt verstrekt in verband met de uitvoering van de Hoofdovereenkomst.
Kritische Derde	een Derde die goederen levert, danwel diensten of werkzaamheden verricht die zodanig essentieel zijn, dat het niet beschikbaar zijn daarvan direct leidt dan wel kan leiden tot het onderbreken of beperken van de distributie van warmte, elektriciteit of gas.
Least Privilege Principe	een beveiligingsconcept en operationele maatregel waarbij elke gebruiker, proces of systeem binnen de organisatie c.q. het domein slechts die toegangsrechten en permissies krijgt die noodzakelijk zijn om de voor die gebruiker, proces of systeem essentiële taken en functies uit te kunnen voeren.
Persoonsgegevens	alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"), zoals nader gespecificeerd in artikel 4 lid 1 van de AVG.
Station	een fysieke locatie in de Infrastructuur van Enexis, waar apparatuur is gehuisvest voor het transport en/of de distributie van elektriciteit, gas (een tot het elektriciteitsnet of gastransportnet van Enexis Netbeheer B.V. behorend transformator-, schakel-, verdeel- en onderstation, installatie of hulpmiddel), zoals bedoeld in artikel 1 sub i Elektriciteitswet en artikel 1 sub d Gaswet dan wel in de nieuwe

	Energiewet.
Toegangsbeveiliging	het op gecontroleerde wijze verlenen van toegang aan geautoriseerde personen of systemen, waarbij toegang door ongeautoriseerde personen of systemen voorkomen wordt door het treffen van technische maatregelen.
Vertrouwelijke Informatie	Informatie waarvan het vertrouwelijke karakter door Enexis uitdrukkelijk is medegedeeld of dit vertrouwelijke karakter redelijkerwijs aangenomen moet worden op grond van de aard en inhoud. Deze informatie ziet in ieder geval op de beveiliging van Enexis.
Werkzaamheden	in afwijking van de AV ziet dit begrip op alle door Wederpartij op basis van de Hoofdovereenkomst uit te voeren activiteiten.

1. DOEL, TOEPASSELIJKHEID EN HIËRARCHIE

1.1 Dit DV&P Addendum heeft tot doel om in aanvulling op de Hoofdovereenkomst afspraken te maken over de minimaal te treffen Beveiligingsmaatregelen en verantwoordelijkheden van Partijen.

1.2 Dit DV&P Addendum is van toepassing op:

a) alle Werkzaamheden, goederen en/of diensten die Wederpartij op basis van de Hoofdovereenkomst voor Enexis uitvoert en zal uitvoeren en/of aan Enexis levert en zal leveren;

b) alle relevante c.q. betrokken Informatie, processen, goederen en diensten van Enexis die aan Wederpartij worden verstrekt respectievelijk waarmee Wederpartij door uitvoering van de Hoofdovereenkomst bekend is geworden

1.3 De verplichtingen van Wederpartij op basis van dit DV&P Addendum gelden, voor zover relevant, tevens ten aanzien van Enexis Holding N.V. en alle tot haar groep behorende bedrijven.

1.4 Afwijkingen van dit DV&P Addendum gelden slechts als deze schriftelijk tussen Partijen zijn overeengekomen in **Bijlage 1 - Overeengekomen afwijkingen van DV&P Addendum**.

1.5 In het geval van tegenstrijdigheden tussen dit DV&P Addendum en de Hoofdovereenkomst, prevaleert hetgeen is opgenomen in dit DV&P Addendum tenzij in de Hoofdovereenkomst nadrukkelijk van een artikel uit dit DV&P Addendum wordt afgeweken.

2. BEVEILIGINGSBELEIDSLIJNEN

2.1 Wederpartij garandeert dat alle Werkzaamheden, goederen en/of diensten onder de Hoofdovereenkomst, waaronder begrepen deelopleveringen, telkens voldoen aan voor Enexis toepasselijke en meest actuele wet- en regelgeving en gangbare normen op het gebied van beveiliging. Hieronder wordt minimaal begrepen:

Wetgeving

a) de NIS2-richtlijn zoals geïmplementeerd in de Cyberbeveiligingswet;
b) de CER-richtlijn zoals geïmplementeerd in de Wwke;
c) de Energiewet, waaronder in het bijzonder artikel 3.18 Energiewet;
d) de Netcode voor Digitale Veiligheid; en
e) de AVG.

Relevante normen

f) ISO 27001, NIST 800-53 of daaraan gelijkwaardige normen; en
g) de ICT-Beveiligingsrichtlijnen vanuit het Nationaal Cyber Security Centrum.

2.2 Wederpartij garandeert verder dat alle Werkzaamheden, goederen en/of diensten onder de Hoofdovereenkomst, waaronder begrepen deelopleveringen, voldoen aan de gestelde eisen in de Bijlagen:

Bijlage 4 - Toegangsbeveiliging
Bijlage 5 - Encryptie & back-ups
Bijlage 6 - Personele en fysieke beveiliging
Bijlage 7 - Training en bewustzijn
Bijlage 8 - Patchmanagement
Bijlage 9 - Vulnerability management
Bijlage 10 - Continuïteitsbeheer
Bijlage 11 - Softwareontwikkeling
Bijlage 12 - Logging & Beveiligingscontroles

Paraaf Enexis Paraaf Wederpartij

2.3 Wederpartij beschikt over een onafhankelijk gecertificeerd kwaliteitssysteem voor beveiliging (ISO 27001, ISO 9001 of gelijkwaardig) dat voldoet aan de eisen van de Plan-Do-Check-Act cyclus. Dit kwaliteitssysteem moet gericht zijn op de bescherming van alle Werkzaamheden, goederen en/of diensten die Wederpartij levert aan dan wel inzet ten behoeve van Enexis.

2.4 Wederpartij implementeert tijdig maatregelen conform ISO 27001 of gelijkwaardig om de beveiliging te waarborgen. Deze Beveiligingsmaatregelen omvatten technische, fysieke en organisatorische maatregelen waarbij minimaal is geïmplementeerd:

a) (security) risico management, waaronder beleid en procedures voor het beoordelen van de effectiviteit van maatregelen;
b) adequate fysieke bescherming van relevante gebouwen en infrastructuur;
c) incidentvoorkoming en -afhandeling en het herstel daarvan;
d) business continuity maatregelen, waaronder business continuity management, back-up management, disaster recovery en crisis management;
e) beveiliging van de keten van Wederpartij (lees: in relatie tot Derden);
f) beveiliging bij de aanschaf, ontwikkeling en onderhoud van netwerk- en informatiesystemen;
g) bewustwording en training van medewerkers op het gebied van beveiliging;
h) logische Toegangsbeveiliging, waaronder de toepassing van multi-factor authenticatie en logging;
i) personele bescherming, waaronder fysieke toegang en bescherming van bedrijfsmiddelen.

2.5 Wederpartij houdt adequate documentatie en een overzicht bij van alle getroffen Beveiligingsmaatregelen zoals bedoeld in dit DV&P Addendum en verstrekt op verzoek een kopie daarvan aan Enexis.

3. GEHEIMHOUDING EN VERWERKING VAN GEGEVENS

3.1 In aanvulling op artikel 12.1 AV, geldt met betrekking tot Vertrouwelijke Informatie en Persoonsgegevens dat Wederpartij Informatie uitsluitend voor de uitvoering van de Hoofdovereenkomst mag gebruiken en deze niet bekend maakt, kopieert, reproduceert of voor eigen doeleinden gebruikt zonder voorafgaande toestemming van Enexis.

3.2 Indien Enexis aan Wederpartij toestemming verstrekt, mag deze Informatie slechts aan die personen voor wie toestemming verkregen is openbaar worden gemaakt met inachtneming van de overige voorwaarden zoals gesteld in dit DV&P Addendum en met dien verstande dat hij de verkregen Informatie op geen enkele wijze aan derden openbaar maken, kopiëren, reproduceren en/of verspreiden.

3.3 De verplichtingen uit artikel 3.1 en artikel 3.2 van dit DV&P Addendum zijn niet van toepassing op Informatie die op het moment van verstrekken door Enexis openbaar is en/of die op grond van een wettelijke bepaling of voorschrift openbaar gemaakt moet worden, mits Partijen voorafgaand de voorgestelde vorm, het tijdspad, de aard en het doel van de bekendmaking hebben afgestemd.

3.4 Op schriftelijk verzoek van Enexis en/of na afloop van de Hoofdovereenkomst, geeft Wederpartij alle door Enexis verstrekte goederen die Informatie bevatten terug. Wederpartij retourneert zo spoedig mogelijk, en zonder het houden van kopieën, alle Informatie en verwijdert deze vervolgens onherstelbaar, tenzij hij op grond van een wettelijk voorschrift gehouden is bepaalde Informatie te bewaren. Op verzoek van Enexis geeft Wederpartij een schriftelijke verklaring af waarin hij bevestigt deze verwijdering te hebben uitgevoerd, en welke Informatie hij eventueel nog bewaart op grond van een wettelijk voorschrift. Wederpartij retourneert de Informatie aan Enexis in een bestandsformaat dat door Enexis kan worden ingelezen en zorgt hierbij dat de integriteit en bruikbaarheid van de Informatie gewaarborgd blijft.

3.5 Deze verplichting tot geheimhouding geldt vanaf het moment van ondertekening van de Hoofdovereenkomst en is van toepassing tot tien (10) jaar na het eindigen daarvan.

3.6 Als Partijen bij de uitvoering van de Hoofdovereenkomst overeenkomstig artikel 22.2 AV een Verwerkersovereenkomst hebben gesloten, zal in het geval van tegenstrijdigheden tussen dit DV&P Addendum en die Verwerkersovereenkomst, hetgeen is opgenomen in de Verwerkersovereenkomst prevaleren.

Paraaf Enexis Paraaf Wederpartij

3.7 Tenzij Enexis hiervoor specifieke toestemming heeft verleend, zal Wederpartij in de uitvoering van de Hoofdovereenkomst geen Informatie verwerken in c.q. verstrekken aan landen buiten de Europese Economische Ruimte. Wederpartij houdt in **Bijlage 3 - Locaties Informatie** een centraal overzicht bij van alle verwerkingslocaties. Dit overzicht bevat de naam, het adres en het land van de verwerkingslocatie, ook voor zover sprake is van de inschakeling van een Derde. In het geval van wijzigingen voorziet Wederpartij Enexis zo spoedig mogelijk, maar uiterlijk binnen één (1) maand na wijziging, met een nieuwe versie.

3.8 Wederpartij treft in overeenstemming met instructies van Enexis passende en erkende maatregelen om verouderde Informatie automatisch te verwijderen dan wel te anonimiseren. Daar waar Informatie nog niet wordt verwijderd of geanonimiseerd, wordt deze waar nodig door Wederpartij gemaskeerd of gepseudonimiseerd in overeenstemming met de Guidelines 01/2025 van de European Data Protection Board.

4. AUDIT

4.1 In aanvulling op artikel 11.2 en 11.3 AV, geldt tussen Partijen dat Enexis het recht heeft periodiek toe te (laten) zien op de naleving van dit DV&P Addendum door Wederpartij middels een audit door een onafhankelijke derde partij waarbij de opdracht wordt uitgevoerd door een EDP auditor welke geaccrediteerd is door NOREA of gelijkwaardig. Wederpartij treft verder contractuele regelingen met zijn toeleveranciers doe door Enexis zijn aangewezen als Kritische Derde(n) die voorzien in een dergelijk auditrecht voor Enexis en die doorwerken in de hele toeleveringsketen.

4.2 Wederpartij verleent de auditor onbelemmerde toegang tot de relevante systemen, documenten en locaties die nodig zijn voor een volledige en effectieve audit. Daarnaast verstrekt hij binnen een redelijke termijn alle relevante informatie, documentatie en rapportages. Indien verbeterpunten en/of tekortkomingen worden geïdentificeerd, documenteert Wederpartij deze en treft hij de noodzakelijke correctieve- en preventieve maatregelen. Indien verbeterpunten en/of tekortkomingen een (in)direct risico voor Enexis introduceren, treft Wederpartij uiterlijk binnen één (1) maand de noodzakelijke correctieve- en preventieve maatregelen.

4.3 Partijen gaan vertrouwelijk om met auditbevindingen en informatie tijdens de audit verkregen, tenzij een toezichthoudende instantie openbaarmaking vereist.

4.4 De kosten van een audit worden gedragen door Enexis, tenzij uit de audit blijkt dat Wederpartij ernstig tekort geschoten is in de nakoming van dit DV&P Addendum, in welk geval Wederpartij verplicht is de kosten geheel of gedeeltelijk te vergoeden.

4.5 Enexis heeft het recht om periodiek algemeen aanvaarde en gangbare geautomatiseerde controles, bijvoorbeeld door middel van third party risk management software, uit te voeren op Wederpartij op basis van openbare bronnen. Deze controles worden zodanig uitgevoerd dat zij geen verstoring van de bedrijfsactiviteiten van Wederpartij veroorzaken. Enexis meldt eventuele geconstateerde afwijkingen die een impact hebben op de uitvoering van de Hoofdovereenkomst aan Wederpartij, voorzien van gedetailleerde informatie over de aard van de afwijking, de mogelijke risico's en aanbevelingen voor corrigerende maatregelen. Wederpartij geeft binnen 30 dagen na schriftelijke melding door Enexis bij Enexis aan hoe hij geconstateerde risico’s zal mitigeren en welke corrigerende maatregelen hij doorvoert.

4.6 Wederpartij beschikt gedurende de gehele looptijd van de Hoofdovereenkomst over een geldige ISAE 3000- of SOC2 type 2 derdenverklaring (Third Party Mededeling) of ISO 27001 (of daaraan gelijkwaardig) certificaat, dat specifiek ziet op de goederen, diensten en/of Werkzaamheden onder de Hoofdovereenkomst en verstrekt hiervan binnen één (1) maand na verzoek een afschrift aan Enexis.

5. COMMUNICATIE EN RAPPORTAGE

5.1 **Bijlage 2 - Contactpersonen** bevat een lijst van contactpersonen die in specifieke situaties verplicht benaderd moeten worden door de andere Partij. Bijvoorbeeld in het geval van een Incident zoals bedoeld in artikel 6 van dit DV&P Addendum.

Paraaf Enexis Paraaf Wederpartij

5.2 In aanvulling op artikel 44.1 AV geldt dat Wederpartij een proactieve houding aanneemt op het gebied van beveiliging. Wederpartij communiceert open en proactief en minimaal vier (4) keer per jaar over ontwikkelingen en bedreigingen op het gebied van beveiliging die mogelijk invloed hebben op Enexis.

5.3 In aanvulling op artikel 43 AV rapporteert Wederpartij halfjaarlijks aan Enexis over de gemaakte afspraken in dit DV&P Addendum. Deze rapportage bevat minimaal:

a) een review van de algemene conclusies en kritieke bevindingen van beveiligingscontroles, waaronder van penetratietesten, interne en externe audits en security logs;
b) een review van Incidenten die hebben plaatsgevonden;
c) lopende en verwachte ontwikkelingen inzake de Werkzaamheden, goederen en/of diensten onder de Hoofdovereenkomst met een impact op de Beveiliging en/of de certificering van Wederpartij;
d) een evaluatie van de effectiviteit van Beveiligingsmaatregelen die zijn beschreven in Bijlage 4 tot en met 12;
e) relevante dreigingen en risico's op het gebied van beveiliging; en
f) updates met betrekking tot naleving van wet- en regelgeving.

6. INCIDENTRESPONSE EN MELDINGSPLICHT

6.1 In aanvulling op artikel 38 AV geldt dat Wederpartij actief monitort op Incidenten en eventuele inbreuken op de getroffen Beveiligingsmaatregelen en over de resultaten daarvan aan Enexis rapporteert in overeenstemming met dit artikel.

6.2 Wederpartij verleent op verzoek van Enexis alle noodzakelijke bijstand bij de nakoming van toepasselijke wet- en regelgeving op het gebied van Beveiliging, waaronder begrepen ondersteuning bij activiteiten en informatieverzoeken van de toezichthouder(s), bevoegde autoriteit(en) en betrokkene(n).

6.3 Wanneer zich (vermoedelijk) een Incident voordoet of heeft voorgedaan, is Wederpartij aanvullend op artikel 38.1 AV verplicht de contactpersonen van Enexis genoemd in **Bijlage 2** via de benoemde communicatiemiddelen onmiddellijk, doch uiterlijk binnen 12 uur, in kennis te stellen en daarbij alle relevante informatie te verstrekken over:

a) het vermoedelijke tijdstip van de aanvang van het Incident;
b) zo mogelijk, een prognose van de hersteltijd;
c) de aard van het Incident;
d) de geconstateerde en vermoedelijke gevolgen van het Incident; en
e) de maatregelen die zijn getroffen of worden getroffen om het Incident op te lossen dan wel de gevolgen c.q. schade zoveel mogelijk te beperken en herhaling te voorkomen.

6.4 Wederpartij is in aanvulling op artikel 38.2 AV verplicht om maatregelen te treffen die redelijkerwijs van hem verwacht kunnen worden om het Incident zo snel mogelijk te herstellen, de verdere gevolgen zoveel mogelijk te beperken en herhaling te voorkomen. Wederpartij treedt zonder uitstel in overleg met Enexis teneinde hierover nadere afspraken te maken.

6.5 Wederpartij verleent Enexis te allen tijde medewerking, volgt de instructies van Enexis op en verricht deugdelijk onderzoek naar het Incident. Wederpartij stelt een rapportage op over het Incident, inclusief een correcte respons en passende vervolgstappen. Deze rapportage deelt Wederpartij zo spoedig mogelijk met Enexis.

6.6 In aanvulling op artikel 38.3 AV is het Wederpartij niet toegestaan informatie te verstrekken aan derde partijen over Incidenten, tenzij Wederpartij daartoe wettelijk verplicht is.

6.7 Wederpartij houdt een register bij van plaatsgevonden Incidenten en inbreuken op de getroffen Beveiligingsmaatregelen.

7. RELATIES MET DERDEN

7.1 In aanvulling op artikel 20 AV geldt dat Wederpartij bij de selectie van een Derde een due diligence proces volgt om zijn geschiktheid te valideren op basis van de mate waarin die Derde kan voldoen aan de Beveiligingsmaatregelen in dit DV&P Addendum. Wanneer blijkt dat een Derde (op delen) niet kan voldoen aan de overeengekomen Beveiligingsmaatregelen en/of hoge risico's introduceert op het gebied van beveiliging, continuïteit en/of privacy, kan de betreffende Derde alleen met voorafgaande toestemming van Enexis worden ingezet. Wederpartij stelt in dit due diligence proces door middel van een risicobeoordeling zoals bedoeld in ISO 27005 dan wel ISO 31000 vast of sprake is van een Kritische Derde.

7.2 Indien Wederpartij een Derde inschakelt voor de uitvoering van (een onderdeel van) de Hoofdovereenkomst, legt Wederpartij door middel van een schriftelijke overeenkomst zoals bedoeld in artikel 20.2 AV aan deze Derde minimaal dezelfde verplichtingen op als die op grond van dit DV&P Addendum voor Wederpartij gelden. Wederpartij blijft jegens Enexis volledig verantwoordelijk voor de wijze waarop deze Derde hieraan uitvoering geeft.

7.3 Wederpartij voert in aanvulling op artikel 11 AV periodiek, minimaal één (1) keer per jaar, audits en beoordelingen uit bij Derde(n) om te verzekeren dat zij voldoen aan overeengekomen Beveiligingsmaatregelen, waaronder begrepen een controle op het incident respons proces. De resultaten van deze audits en beoordelingen worden gedocumenteerd en Wederpartij ziet erop toe dat eventuele tekortkomingen worden aangepakt met corrigerende maatregelen.

7.4 Wederpartij verplicht Kritische Derde(n) om continuïteitsplannen en -procedures te ontwikkelen en te onderhouden om de continuïteit en het herstel van levering van producten en diensten te waarborgen in geval van incidenten of verstoringen. Een dergelijk continuïteitsplan voldoet minimaal aan de eisen uit **Bijlage 10**.

7.5 Wederpartij houdt een up-to-date overzicht bij van de Derde(n) die zij inzet voor de uitvoering van de Hoofdovereenkomst, waaronder inbegrepen een demarcatie van zijn Werkzaamheden ten opzichte die van andere relevante systemen en applicaties.

8. DUUR EN BEEINDIGING

8.1 Het DV&P Addendum treedt, voor zover nodig met terugwerkende kracht, in werking op het moment van rechtsgeldige ondertekening door Partijen van de Hoofdovereenkomst. Het DV&P Addendum eindigt van rechtswege op het moment van eindigen van de Hoofdovereenkomst, met dien verstande dat altijd voldaan zal moeten worden aan het bepaalde in artikel 48 AV.

8.2 De bepalingen uit DV&P Addendum die de strekking hebben om na beëindiging van het DV&P Addendum te blijven gelden, blijven na het eindigen daarvan voor de aanvullende duur van tien (10) jaar van kracht. Dit betreft in ieder geval de artikelen Geheimhouding en verwerking gegevens (artikel 3) en dit artikel.

9. TUSSENTIJDSE BEËINDIGING, ONTBINDING EN OPSCHORTING

9.1 Enexis heeft in aanvulling op artikel 18.1 en 18.4 AV het recht om de Hoofdovereenkomst per direct, zonder ingebrekestelling en zonder rechtelijke tussenkomst op te schorten, te ontbinden danwel op te zeggen en de door Enexis geleden schade vergoed te krijgen in het geval van:

a) schending van artikel 2, artikel 3 en/of artikel 6 van dit DV&P Addendum door Wederpartij.

9.2 Buiten een vergoeding voor in redelijkheid gemaakte, onvermijdbare kosten voor reeds in productie genomen goederen of onderhanden werk, geeft ontbinding of opzegging van de Hoofdovereenkomst op basis van dit DV&P Addendum Wederpartij geen recht op verdere vergoeding van enigerlei schade.

Paraaf Enexis

Paraaf Wederpartij

10. VERZEKERING

10.1 Wederpartij is in het bezit van een adequate zakelijke verzekering voor cybersecurity. Het verzekerd bedrag van de zakelijke verzekering voor cybersecurity bedraagt minimaal [EUR 2.500.000][1] per gebeurtenis. Op verzoek van Enexis verstrekt Wederpartij de betreffende polisvoorwaarden en/of het bewijs van verzekeringsdekking hiervan.[2]

11. OVERIG

11.1 Enexis is gerechtigd wijzigingen in het DV&P Addendum door te voeren die wegens gewijzigde inzichten, toepasselijke wet- en regelgeving, gewijzigde omstandigheden en/of risico's noodzakelijk zijn.

> *Toelichting: De ontwikkelingen en inzichten op het gebied van Cybersecurity volgen zich in een snel tempo op. Inherent aan deze ontwikkeling is dat de (beveiligings)maatregelen als beschreven in de Bijlagen telkens worden geëvalueerd en doorontwikkeld. Bij Enexis is gebruikelijk dat alvorens wijzigingen in één van deze Bijlagen worden doorgevoerd, dat dit niet wordt doorgevoerd zonder goed overleg met Wederpartij.*

11.2 Wijzigingen door Enexis in dit DV&P Addendum geven Wederpartij aanspraak op bijbetaling, voor zover hij aantoont dat door die wijziging aanzienlijk meer wordt gevraagd, dan redelijkerwijs van hem kan worden gevergd.

11.3 Enexis heeft onverkort een recht tot opschorting zoals bedoeld in artikel 6:52 BW voor zover sprake is van een tekortkoming van Wederpartij in de nakoming van zijn verplichtingen in het DV&P Addendum.

Aldus overeengekomen te <plaats> en ondertekend:

<datum>	<datum>
Enexis Personeel B.V./Enexis Netbeheer B.V.]	<naam Wederpartij>
<Ondertekenaar Enexis>	<Ondertekenaar Wederpartij>
<Functie>	<Functie>

1 Voor de invulling van dit bedrag wordt door het CISO/CLA afstemming gezocht met een verzekeringsexpert.
2 Voor aansprakelijkheid en vrijwaring wordt aangesloten bij de Hoofdovereenkomst.

Paraaf Enexis Paraaf Wederpartij

BIJLAGEN

1. Overeengekomen afwijkingen van DV&P Addendum
2. Contactpersonen
3. Locaties Informatie
4. Toegangsbeveiliging
5. Encryptie en back-ups
6. Personele en fysieke beveiliging
7. Training en bewustzijn
8. Patchmanagement
9. Vulnerability management
10. Continuïteitsbeheer
11. Softwareontwikkeling
12. Logging & Beveiligingscontroles

Paraaf Enexis

Paraaf Wederpartij

BIJLAGE 1 – OVEREENGEKOMEN AFWIJKINGEN DV&P ADDENDUM

Partijen zijn overeengekomen de tekst van het DV&P Addendum op de volgende punten te wijzigen:

Art.	Tekst die vervalt	Vervangende tekst	Reden

Paraaf Enexis

Paraaf Wederpartij

BIJLAGE 2 – CONTACTPERSONEN

Wanneer zich een inbreuk en/of Incident voordoet of heeft voorgedaan en/of indien sprake is van een kwetsbaarheid die een direct risico voor Enexis vormt, is Wederpartij verplicht hiervan melding te doen via **Security@enexis.nl** en via de telefoonnummers van de contactpersonen van Enexis genoemd in **Bijlage 2.** Wederpartij dient Enexis hier via alle benoemde communicatiemiddelen onmiddellijk, doch uiterlijk binnen 12 uur nadat Wederpartij daar kennis van heeft genomen, van in kennis te stellen en daarbij alle relevante informatie te verstrekken:

Contactinformatie van **Enexis**

Gebeurtenis	Naam	Functie	Telefoon nummer
Incident en inbreuk	Jeroen Teppema	Chief Information Security Officer	088-8574444
Incident en inbreuk		Contract verantwoordelijke Hoofdovereenkomst	
Privacy Incident en inbreuk	Evelyne Hengst-de Greeff	Functionaris Gegevensbescherming	088-8574444

Contactinformatie van **Wederpartij**

Gebeurtenis	Naam	Functie	Telefoon nummer	E-mail
Incident en inbreuk		Chief Information Security Officer		
Incident en inbreuk		Contract verantwoordelijke Hoofdovereenkomst		
Incident en inbreuk		Functionaris Gegevensbescherming		

Paraaf Enexis

Paraaf Wederpartij

BIJLAGE 3 – LOCATIES INFORMATIE

Wederpartij maakt bij de uitvoering van de Hoofdovereenkomst gebruik van de volgende verwerkingslocaties:

Locaties waar Wederpartij Informatie bewaart, verwerkt etc.	Locaties waar Derde(n) Informatie bewaart, verwerkt etc.	Toelichting
[Land, Adres]	[Statutaire naam Derde, Land, Adres]	

Paraaf Enexis

Paraaf Wederpartij

BIJLAGE 4 - TOEGANGSBEVEILIGING

I. Wederpartij beheert de logische toegang tot de ICT-Oplossing en overige diensten van Wederpartij door middel van technische en organisatorische maatregelen. Hieronder wordt minimaal verstaan:

   a) het gebruik van accounts die herleidbaar zijn naar een gebruiker of systeemactiviteit (lees: service accounts);
   b) het toepassen van tweefactor authenticatie op basis van iets wat je weet en iets wat je hebt en/of bent; en
   c) het gebruik van sterke wachtwoorden of een ander authenticatiemiddel welke breed wordt toegepast, betrouwbaar is en als industriestandaard kan worden aangemerkt.

II. Alle toegang tot de ICT-Oplossing en overige diensten wordt door Wederpartij beheerd via een centraal autorisatiesysteem. Dit autorisatiesysteem zorgt voor een consistent en gestandaardiseerd proces voor het verlenen en intrekken van toegangsrechten.

III. Wederpartij garandeert de veilige en effectieve implementatie en het beheer van een Single Sign-On (SSO) oplossing binnen de door hen geleverde ICT-oplossing, die naadloos integreert met het toegangsbeveiligingssysteem van Enexis. Wederpartij zorgt dat de SSO-oplossing compatibel is met de geldende industriestandaarden, inclusief maar niet beperkt tot protocollen zoals SCIM, SAML 2.0 en OAuth 2.0.

IV. Toegangsrechten binnen de ICT-Oplossing en overige diensten worden toegewezen op basis van rollen. Iedere rol beschrijft een set verantwoordelijkheden en de daarbij behorende toegangsrechten. Het uitgangspunt bij het opstellen van de rollen is het Least Privilege Principe. Wederpartij beschikt over een gedocumenteerd overzicht van de standaardrollen die binnen de ICT-Oplossing en overige diensten worden toegepast.

V. Wederpartij beoordeelt periodiek, minstens één keer per zes (6) maanden, de toegangsrechten tot de ICT-Oplossing en overige diensten. Deze beoordeling richt zich op de juistheid van de toegewezen rechten en bevestigt dat deze nog steeds in lijn zijn met de huidige rol(len) en verantwoordelijkheden van de gebruikers van Wederpartij. Eventuele afwijkingen of ongeautoriseerde rechten corrigeert Wederpartij onmiddellijk gecorrigeerd. Deze periodieke controle wordt gedocumenteerd, inclusief bevindingen en genomen acties

Paraaf Enexis Paraaf Wederpartij

BIJLAGE 5 – ENCRYPTIE EN BACK-UPS

I. Wederpartij past passende en erkende encryptiemethoden toe om de vertrouwelijkheid en integriteit van Informatie te beschermen tegen onbevoegde toegang, verlies, of wijziging. De geselecteerde encryptiemethoden voldoen aan de geldende industrie standaarden en wettelijke vereisten. Encryptiesleutels worden opgeslagen en beheerd volgens best practices voor sleutelbeheer, zoals vastgelegd in ISO 11770 (of gelijkwaardig), inclusief periodieke rotatie en controle van sleutels. Toegang tot versleutelde Informatie wordt strikt gecontroleerd en gelogd.

II. De Informatie die wordt verwerkt in en wordt overgedragen tussen systemen c.q. applicaties, zowel binnen als buiten het netwerk van Wederpartij, wordt versleuteld conform de eisen in het vorige artikel om deze Informatie te beschermen tegen onderschepping en manipulatie. Dit omvat, maar is niet beperkt tot, gegevensoverdracht via e-mail, API's, netwerken, en clouddiensten.

III. Ten behoeve van het bestrijden van calamiteiten maakt Wederpartij dagelijks, of vaker indien nodig, reservekopieën (back-ups) van de Informatie om herstel van Informatie binnen de afgesproken RPO mogelijk te maken. Wederpartij neemt maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van de back-ups te garanderen. Hieronder wordt verstaan het toepassen van encryptie, het dupliceren van de back-ups naar verschillende gescheiden fysieke locaties en het beschikken over uitwijklocaties. Wederpartij test minimaal één keer per jaar de back-up aantoonbaar op werking door het uitvoeren van een hersteltest (recovery test) en deelt de resultaten van deze test met Enexis. Indien de test niet geslaagd is, voert Wederpartij correctieve maatregelen en de test binnen één (1) maand opnieuw uit.

Paraaf Enexis Paraaf Wederpartij

BIJLAGE 6 – PERSONELE EN FYSIEKE BEVEILIGING

I. Enexis kan de werknemers van Wederpartij dan wel andere door Wederpartij voor de uitvoering van de Hoofdovereenkomst ingezette derden, aan een veiligheidsonderzoek onderwerpen voor zover dit wettelijk is toegestaan. Wederpartij verleent aan dat onderzoek zijn volledige medewerking. Enexis kan op grond van de uitkomsten daarvan de inzet van de betrokken werknemer en/of derde bij de uitvoering van de Hoofdovereenkomst weigeren.

II. Indien als onderdeel van de Hoofdovereenkomst mogelijk medewerkers en/of derden van Wederpartij zelfstandig fysieke toegang hebben tot locaties van Enexis, waaronder Stations, dan gelden de volgende bepalingen:

a) Wederpartij verstrekt toegangsmiddelen, die gerelateerd zijn aan de dienstverlening aan Enexis, enkel aan zijn medewerkers en derden conform de daarvoor geldende Enexis procedures, indien en zo lang zij dit nodig hebben voor de uitvoering van hun Werkzaamheden;
b) eventuele toegangsmiddelen, waaronder gebruikersaccounts die Enexis aan medewerkers van Wederpartij verstrekt zijn strikt persoonsgebonden en mogen niet overgedragen worden aan een andere persoon;
c) in het kader van security en veiligheid worden medewerkers en derden van Wederpartij bij het betreden van Enexis locaties altijd begeleid door Enexis medewerkers;
d) Wederpartij leeft door Enexis verstrekte en op de website van Enexis gepubliceerde gedragscodes en huisregels met betrekking tot de veiligheid van de toegang tot Enexis locaties en hulpmiddelen na;
e) wanneer voor een medewerker of derde van Wederpartij fysieke toegang dan wel gebruik van Enexis hulpmiddelen, waaronder begrepen laptops, niet meer noodzakelijk is, dan staat Wederpartij ervoor in te staan dat deze hulpmiddelen en de toegangsmiddelen weer door die medewerker of derde worden ingeleverd conform de daarvoor geldende Enexis procedures op uiterlijk de dag dat desbetreffende medewerker of derde de laatste werkzaamheden voor Enexis heeft verricht.

III. Indien Wederpartij gebruik maakt van door Enexis beschikbaar gestelde IT-middelen en beheer- en systeemaccounts (of andere technische mogelijkheden), gebruikt Wederpartij deze niet voor andere doeleinden dan het uitvoeren van de Hoofdovereenkomst. Eventuele wachtwoorden houdt Wederpartij geheim en beveiligt hij adequaat en de kring van individuen die toegang heeft tot de wachtwoorden beperkt Wederpartij tot die personen die toegang nodig hebben voor het uitvoeren van de Hoofdovereenkomst.

IV. Wanneer medewerkers van Wederpartij toegang krijgen tot applicaties en systemen van Enexis op basis van federatie, moeten zij zich registreren en communiceren via zakelijke e-mailadressen die aan hun organisatie zijn gekoppeld. Het gebruik van persoonlijke e-mailadressen, zoals Gmail, Hotmail, Yahoo, en vergelijkbare diensten, is niet toegestaan.

Paraaf Enexis Paraaf Wederpartij

BIJLAGE 7 – TRAINING EN BEWUSTZIJN

I. Wederpartij zet een trainings- en bewustwordingsprogramma op waarmee hij zijn medewerkers en derden periodiek opleidt over ontwikkelingen, bedreigingen en toepasselijke wet- en regelgeving op het gebied van Beveiliging. In het trainings- en bewustwordingsprogramma wordt minimaal aandacht gegeven aan de volgende onderwerpen:

a) herkennen en melden van phising en andere digitale dreigingen;
b) fysieke toegang;
c) veilig omgaan met en uitwisselen van Vertrouwelijke Informatie;
d) gebruik van sterke wachtwoorden, tweefactorauthenticatie en wachtwoordmanagers;
e) veilig gebruik van end user devices (bijvoorbeeld laptops en telefoons) en netwerken;
f) en indien relevant, het veilig ontwikkelen van software.

II. Afhankelijk van het risicoprofiel van de betreffende medewerkers en/of derden en de aard van de Werkzaamheden die zij verrichten en/of de goederen en/of diensten die zij leveren, biedt Wederpartij hen een specifiek training- en bewustwordingsprogramma aan.

III. De training wordt verzorgd door een onafhankelijke en gekwalificeerde trainer die beschikt over:

a) aantoonbare ervaring met beste praktijken op het gebied van netwerk- en informatiebeveiliging;
b) kennis van nationale, Europese en internationale standaarden op het gebied van netwerk- en informatiebeveiliging;
c) kennis van mogelijke maatregelen en oplossingen voor risico's als bedoeld in artikel 20 Cyberbeveiligingswet; en
d) kennis van netwerk- en informatiebeveiligingsvraagstukken op strategisch en tactisch niveau.

BIJLAGE 8 – PATCHMANAGEMENT

I. Wederpartij is verplicht om tijdens de looptijd van de Hoofdovereenkomst periodiek patches en updates beschikbaar te stellen om bekende (beveiliging)fouten in de ICT-Oplossing, waaronder begrepen de onderliggende IT-infrastructuur, systemen en/of Informatie van Enexis, te verhelpen.

II. De frequentie van het patchen wordt risico gebaseerd uitgevoerd door Wederpartij, waarbij dit minimaal één (1) keer per maand gebeurt. In het geval van kritieke beveiligingsupdates is Wederpartij verplicht deze zo spoedig mogelijk uit te voeren, doch uiterlijk binnen drie (3) werkdagen na publicatie van de betreffende update. Wederpartij is verplicht om ten minste één (1) werkdag voorafgaand hieraan een digitale notificatie hierover aan Enexis te versturen.

III. Wederpartij informeert Enexis tijdig over de geplande patches en updates, inclusief de aard van de wijzigingen, de potentiële impact op de ICT-Oplossing en/of diensten en de verwachte onderbreking. Dit dient te geschieden via digitale notificatie ten minste zeven (7) werkdagen voorafgaand aan de beoogde installatie datum.

IV. Het doorvoeren van patches en updates wordt door Wederpartij zoveel mogelijk binnen de, bijvoorbeeld in de Service Level Agreement, vastgestelde onderhoudsvensters gedaan, zodat de impact op de operationele processen van Enexis tot een minimum wordt beperkt. Uitzonderingen hierop zijn kritieke patches, die onmiddellijk geïnstalleerd moeten worden om de veiligheid en integriteit van de ICT-Oplossing te waarborgen.

V. Voor de uitrol van software patches dient Wederpartij grondige tests uit te voeren in een testomgeving die representatief is voor de productieomgeving. De tests moeten ten minste de volgende aspecten dekken:

   a) de (Functionele) werking van de ICT-Oplossing;
   b) de impact op bestaande functionaliteit; en
   c) de Beveiligingsaspecten.

VI. Wanneer Enexis zelf verantwoordelijk is voor het installeren van de door Wederpartij beschikbaar gestelde patches en updates, dient Enexis ervoor te zorgen dat deze patches en updates tijdig worden geïnstalleerd. Wederpartij is verplicht om Enexis tijdig, binnen vijf (5) werkdagen na het beschikbaar komen van de patches en updates, informatie hierover te verstrekken aan Enexis.

Paraaf Enexis Paraaf Wederpartij

BIJLAGE 9 – VULNERABILITY MANAGEMENT

I. Wederpartij is verplicht om tijdens de looptijd van de Hoofdovereenkomst een vulnerability management programma te implementeren en te onderhouden. Dit programma moet gericht zijn op het identificeren, evalueren en verhelpen van beveiligingskwetsbaarheden in de onder de verantwoordelijkheid van Wederpartij vallende systemen, netwerken en software die worden ingezet voor de uitvoering van de Hoofdovereenkomst, waaronder begrepen demarcaties met applicaties en systemen van derden.

II. Wederpartij voert periodieke kwetsbaarheidsscans en penetratietests uit op alle relevante systemen en software. Kwetsbaarheidsscans moeten minimaal maandelijks worden uitgevoerd en penetratietest jaarlijks, of vaker indien vereist gezien het risico.

III. Wederpartij is verplicht om de geïdentificeerde kwetsbaarheden te evalueren op basis van hun impact en waarschijnlijkheid. Dit omvat het classificeren van kwetsbaarheden op basis van hun ernst, zoals ‘kritiek’, ‘hoog’, ‘medium’ of ‘laag’ risico conform het Common Vulnerability Scoring System.

IV. Wederpartij verhelpt de geïdentificeerde kwetsbaarheden conform onderstaande hersteltermijnen:

a) Emergency kwetsbaarheden: zo spoedig mogelijk;
b) Kritieke kwetsbaarheden: binnen vijf (5) dagen na identificatie;
c) Hoge kwetsbaarheden: binnen 21 dagen na identificatie;
d) Medium kwetsbaarheden: binnen twee (2) maanden na identificatie;
e) Lage kwetsbaarheden: binnen een redelijke termijn, in overeenstemming met de overeengekomen prioriteiten.

V. Wanneer Enexis verantwoordelijk is voor het verhelpen van kwetsbaarheden informeert Wederpartij Enexis tijdig over de status van kwetsbaarheden, inclusief de aard van de kwetsbaarheden, de potentiële impact, en de stappen die ondernomen moeten worden om deze te verhelpen, en verstrekt hij al de daartoe benodigde hulpmiddelen zoals de vereiste software. Dit gebeurt via een digitale melding ten hoogste binnen vijf (5) werkdagen na de identificatie en evaluatie van de kwetsbaarheden

BIJLAGE 10 - CONTINUITEITSBEHEER

I. Wederpartij is verplicht om binnen twee (2) maanden na ondertekening van de Hoofdovereenkomst een overzichtelijk en gestructureerd bedrijfscontinuïteitsplan op te stellen en ter goedkeuring voor te leggen aan Enexis, waarin minimaal de eisen en processen zoals gecommuniceerd tijdens de eventuele aanbesteding in zijn opgenomen. Dit plan beschrijft hoe de overeengekomen Werkzaamheden, goederen en/of diensten zonder significante onderbreking worden voortgezet door Wederpartij, ook in het geval van uitval, beëindiging of wanprestatie van een Derde(n). Wederpartij waarborgt dat het bedrijfscontinuïteitsplan ten minste de volgende elementen bevat:

a) een volledig overzicht van alle essentiële en relevante processen, systemen en voor Wederpartij relevante Derde(n) in de toeleveringsketen, hun rol en de mate van afhankelijkheid binnen de uitvoering van de Hoofdovereenkomst jegens Enexis en jegens onder verantwoordelijk van Enexis betrokken derden;
b) de kritieke raakvlakken tussen Wederpartij en alle Derde(n) in de toeleveringsketen;
c) de maatregelen die Wederpartij treft om de beschikbaarheid, vertrouwelijkheid en integriteit van Informatie en de continuïteit te waarborgen bij uitval van bijvoorbeeld een relevante Derde;
d) de maximale termijn waarbinnen in geval van uitval van bijvoorbeeld een relevante Derde door Wederpartij een vervangende oplossing is gerealiseerd, al dan niet in de vorm van alternatieve leveranciers of interne capaciteit; en
e) procedures voor het implementeren van redundantie en regelmatige back-ups om de beschikbaarheid en vertrouwelijkheid van de back-ups te garanderen, waaronder het toepassen van versleuteling en het dupliceren van de back-ups naar verschillende gescheiden fysieke locaties;
f) procedures voor het herstel van systemen en data na een incident, inclusief regelmatige tests van het bedrijfscontinuïteitsplan; en
g) procedures en escalatiemechanismen voor communicatie met Enexis bij calamiteiten.

II. Wederpartij is verplicht het bedrijfscontinuïteitsplan periodiek te testen op geschiktheid en minimaal één (1) keer per jaar te herzien en bij wijzigingen meteen een bijgewerkte versie ter goedkeuring aan Enexis voor te leggen. Wederpartij actualiseert in ieder geval dit bedrijfscontinuïteitsplan op het moment dat sprake is van een wijziging of aanvulling van relevante wet- of regelgeving, met inbegrip van enige relevante uitvoeringshandeling van de Europese Commissie en relevante guidance van toezichthoudende autoriteiten.

III. Op verzoek van één van de Partijen vindt met bekwame spoed een coördinatie-overleg plaats, waarbij vertegenwoordigers van Enexis, Wederpartij en voor de bespreking relevante Derde(n) aanwezig zijn. Tijdens dit overleg wordt de voortgang, eventuele Incidenten en verbetermaatregelen besproken.

IV. Wederpartij heeft specifieke maatregelen geïmplementeerd om de risico's van ransomware te beheersen en aanvallen tegen te gaan, waaronder regelmatige back-ups van kritieke gegevens die op veilige, geïsoleerde locaties worden opgeslagen en installatie van anti-malware en andere beveiligingssoftware. In geval van een ransomware-aanval activeert Wederpartij de continuïteitsplannen en stelt een incident respons team samen om de aanval te beoordelen en te beheersen.

BIJLAGE 11 - SOFTWAREONTWIKKELING

Voor zover de uitvoering van de Hoofdovereenkomst door Wederpartij ziet op de ontwikkeling van Software, zijn Partijen het volgende overeengekomen:

I. Wederpartij implementeert beleid en procedures voor de beveiliging van software gedurende de hele ontwikkelcyclus (Software Development Life Cycle).

II. Wederpartij richt een beveiligde ontwikkelomgeving in waarin de ontwikkel-, test-, acceptatie- en productieomgevingen van elkaar gescheiden zijn en de toegang tot broncode en testdata wordt beperkt tot de bij de ontwikkeling betrokken medewerkers en/of contractanten en actief wordt beheerd. Testdata bevat geen Persoonsgegevens en/of Vertrouwelijke Informatie maar geanonimiseerde of gefingeerde gegevens.

III. Wederpartij voorziet de ontwikkelde software uitsluitend van vormen van toegang die door Enexis zijn voorgeschreven of anderszins zijn overeengekomen en brengt geen heimelijke voorzieningen aan ten behoeve van toegang tot de Informatie en/of systemen van Enexis.

IV. Software voor webapplicaties die voor de verwerking van informatie van Enexis en/of derden wordt aangewend, is ontworpen, ontwikkeld, getest en geconfigureerd op basis van gangbare normen voor veilige webapplicaties, waaronder OWASP Top Ten en de Infosheet ICT Beveiligingsrichtlijn voor Webapplicaties van het Nationaal Cyber Security Centrum, of vergelijkbare openbaar beschikbare standaarden.

V. Wederpartij controleert regelmatig de broncode van de ontwikkelde software handmatig en/of met behulp van geautomatiseerde tools (code review) op zwakke plekken, fouten en eventuele risico's.

Paraaf Enexis Paraaf Wederpartij

BIJLAGE 12 – LOGGING & BEVEILIGINGSCONTROLES

I. Wederpartij legt (security) activiteiten en gebeurtenissen vast die invloed kunnen hebben op de integriteit, beschikbaarheid en vertrouwelijkheid van alle vormen van Informatie, processen, goederen en/of diensten van Enexis en van Wederpartij voor zover relevant. Minimaal de volgende activiteiten en gebeurtenissen worden vastgelegd in security logs:

a) pogingen tot systeemtoegang (geslaagde en mislukte inlogpogingen);
b) wijzigingen in systeemconfiguraties en instellingen;
c) acties die zijn ondernomen door gebruikers met verhoogde rechten;
d) incidenten die de beveiliging van systemen en informatie aantasten; en
e) de wijze waarop herhaling wordt voorkomen.

II. Wederpartij verplicht zich om de security logs te beveiligen tegen ongeautoriseerde toegang, wijzigingen, verlies of vernietiging en regelmatig onderhoud te plegen aan de logging-infrastructuur voor optimale prestaties en betrouwbaarheid.

III. Security logs worden voor een minimale periode van zes (6) maanden bewaard, tenzij een verlengde bewaarperiode wettelijk vereist is of noodzakelijk voor lopende onderzoeken. Na afloop van de bewaarperiode worden de gegevens op een veilige en verantwoorde wijze verwijderd.

IV. Wederpartij dient periodiek de effectiviteit van de getroffen Beveiligingsmaatregelen en de mogelijkheid tot herstel van Incidenten te toetsen middels (interne en externe) audits en reviews. Externe audits worden uitgevoerd door onafhankelijke en gekwalificeerde auditeurs. Deze beveiligingscontroles nemen verschillende vormen aan, waaronder kwetsbaarheidsscans van netwerken en systemen, penetratietests, fysieke beveiligingscontroles en toegangscontrolebeheer. De frequentie en aard van deze beveiligingscontroles worden bepaald op basis van de gevoeligheid van de Informatie en de continuïteitsrisico's, waar dit ten minste één (1) keer per jaar plaatsvindt.

V. Indien eventuele verbeterpunten en/of tekortkomingen worden geïdentificeerd, zal Wederpartij deze documenteren en de noodzakelijke correctieve- en preventieve maatregelen treffen. Indien eventuele verbeterpunten en/of tekortkoming een (in)direct risico voor Enexis introduceren, treft Wederpartij uiterlijk binnen één (1) maand de noodzakelijke correctieve- en preventieve maatregelen.

VI. Lessons learned uit beveiligingscontroles en externe audits gebruikt Wederpartij om de Beveiligingsprocedures en -praktijken continu te verbeteren.