Addendum Cybersecuritydiensten Securide B.V.

Artikel 1 – Definities

De in de NLdigital Voorwaarden 2025 gedefinieerde begrippen hebben in dit Addendum dezelfde betekenis, tenzij hieronder anders is bepaald. In dit Addendum wordt voorts verstaan onder:

Penetratietest (Pentest): een geautoriseerd en gecontroleerd onderzoek waarbij Securide actief tracht beveiligingskwetsbaarheden van de in de Scope opgenomen systemen, netwerken of applicaties te identificeren en te exploiteren, met als doel het beveiligingsniveau te beoordelen.

Scope: de uitdrukkelijk en schriftelijk overeengekomen afbakening van systemen, netwerken, applicaties, adressen, technieken, tijdvensters en handelingen waarop een opdracht betrekking heeft, zoals vastgelegd in de Rules of Engagement of in de opdrachtovereenkomst.

Rules of Engagement (RoE): het document dat de Scope, randvoorwaarden, contactpersonen, escalatieprocedure en autorisatie van een penetratietest of vergelijkbare offensieve opdracht vastlegt; de Rules of Engagement maakt deel uit van de opdrachtovereenkomst.

Incident Response (IR): de dienstverlening gericht op het detecteren, beheersen, mitigeren en herstellen van (vermoedelijke) beveiligingsincidenten, alsmede de daarbij behorende advisering en coordinatie.

Forensisch Onderzoek: het onder bewijswaarborgen vergaren, veiligstellen, analyseren en rapporteren van digitale gegevens, mede met het oog op mogelijke juridische procedures of claims.

Forensische Data: alle gegevens, kopieen (images), logbestanden en artefacten die Securide in het kader van Forensisch Onderzoek vergaart of vervaardigt.

Chain of Custody (bewijsketen): de gedocumenteerde keten waaruit blijkt welke Forensische Data wanneer, door wie en op welke wijze zijn vergaard, verwerkt, bewaard en overgedragen, alsmede hoe de integriteit ervan is geborgd.

Kwetsbaarheid: een zwakheid in een systeem, netwerk, applicatie of proces die kan worden misbruikt om de vertrouwelijkheid, integriteit of beschikbaarheid daarvan aan te tasten.

Incident: een gebeurtenis die de beveiliging van gegevens of systemen daadwerkelijk of vermoedelijk in gevaar brengt, daaronder begrepen een incident in de zin van de Cyberbeveiligingswet en een inbreuk in verband met persoonsgegevens in de zin van de AVG.

CVD (Coordinated Vulnerability Disclosure): het gecoordineerd melden van een ontdekte Kwetsbaarheid aan de rechthebbende en/of het NCSC, overeenkomstig de geldende leidraden en gedragscodes.

Opdrachtgever: de wederpartij van Securide, zijnde de klant die handelt in de uitoefening van beroep of bedrijf.

Artikel 2 – Penetratietesten

2.1 Toepasselijkheid van het Scope-begrip

Dit artikel is van toepassing op penetratietesten en daarmee gelijk te stellen offensieve beveiligingsonderzoeken, ongeacht of deze worden uitgevoerd voor een nieuwe of een bestaande opdrachtgever. Elke penetratietest wordt uitsluitend uitgevoerd binnen de schriftelijk overeengekomen Scope, vastgelegd in een door beide partijen ondertekende Rules of Engagement, die deel uitmaakt van de opdrachtovereenkomst.

2.2 Autorisatie

2.2.1 Opdrachtgever verleent Securide uitdrukkelijke toestemming om, gedurende de in de Rules of Engagement omschreven testperiode en binnen de aldaar omschreven Scope, penetratietesten uit te voeren op de aldaar vermelde systemen, netwerken en applicaties.

2.2.2 Securide is uitsluitend gerechtigd te handelen binnen de overeengekomen Scope. Partijen erkennen dat het opzettelijk binnendringen in een geautomatiseerd werk in beginsel strafbaar is op grond van *artikel 138ab van het Wetboek van Strafrecht* (computervredebreuk), en dat de uitdrukkelijke, schriftelijke en voorafgaande toestemming van de rechthebbende de wederrechtelijkheid daarvan opheft. De ondertekende Rules of Engagement vormt deze toestemming.

2.3 Eigendom, bevoegdheid en vrijwaring derde-eigenaren

2.3.1 Opdrachtgever staat ervoor in dat hij de rechthebbende is van alle in de Scope opgenomen systemen, dan wel dat hij de bevoegde toestemming heeft verkregen van alle betrokken derden, waaronder hosting-providers, cloud service providers (zoals AWS, Microsoft Azure en Google Cloud), SaaS-aanbieders en co-locatiebedrijven, wier systemen of infrastructuur deel uitmaken van of bereikbaar zijn vanuit de Scope. Dit sluit aan op artikel 25.1 van de NLdigital Voorwaarden 2025.

2.3.2 Opdrachtgever vrijwaart Securide voor alle aanspraken van derden, daaronder begrepen bestuursrechtelijke sancties van toezichthouders, die voortvloeien uit de uitvoering van de penetratietest in of op systemen waarvoor Opdrachtgever niet de bevoegde toestemming had of heeft verkregen, tenzij Securide aantoonbaar buiten de overeengekomen Scope heeft gehandeld.

2.4 Inherente risico's en aansprakelijkheid tijdens de test

2.4.1 Opdrachtgever erkent dat de uitvoering van penetratietesten inherente risico's met zich meebrengt, waaronder het risico op (tijdelijke) systeemverstoring, verminderde beschikbaarheid van diensten of verlies of beschadiging van data.

2.4.2 Onverminderd artikel 5 van dit Addendum en artikel 15 van de NLdigital Voorwaarden 2025 is Securide niet aansprakelijk voor schade of kosten die het directe of indirecte gevolg zijn van de uitvoering van de penetratietest overeenkomstig de overeengekomen Scope en Rules of Engagement, tenzij die schade is veroorzaakt door opzet of bewuste roekeloosheid van de bedrijfsleiding van Securide.

2.5 Back-upverplichting Opdrachtgever

Opdrachtgever is verantwoordelijk voor het tijdig en volledig maken van back-ups van alle systemen, configuraties en data binnen de Scope voor aanvang van de penetratietest. Het nalaten hiervan komt voor rekening en risico van Opdrachtgever.

2.6 Momentopname en inspanningsverplichting

2.6.1 Een penetratietest betreft een onderzoek naar de beveiligingsstatus van de in de Scope opgenomen systemen op het moment van de test (momentopname). De resultaten bieden geen garantie dat (a) alle Kwetsbaarheden zijn gevonden, (b) de bevindingen na voltooiing van de test nog actueel zijn, of (c) de systemen zijn beschermd tegen toekomstige aanvallen of Kwetsbaarheden.

2.6.2 Securide heeft bij penetratietesten een inspanningsverplichting en geen resultaatsverplichting.

2.7 Escalatie bij kritieke bevindingen

Indien Securide tijdens een penetratietest een kritieke Kwetsbaarheid, een actieve exploit of aanwijzingen voor een lopende aanval door derden ontdekt, schort zij de relevante testhandelingen zo nodig op en informeert zij Opdrachtgever onverwijld via de in de Rules of Engagement opgenomen escalatieprocedure.

Artikel 3 – Incident Response en Forensisch Onderzoek

3.1 Inspanningsverplichting

3.1.1 Securide verleent Incident Response- en Forensisch Onderzoek-diensten op basis van een inspanningsverplichting. Securide garandeert niet dat:

(a) het Incident volledig en definitief zal worden opgelost;

(b) alle oorzaken, vectoren of de volledige omvang van het Incident zullen worden vastgesteld;

(c) herhaling van vergelijkbare Incidenten wordt voorkomen;

(d) systemen of data volledig worden hersteld.

3.1.2 Securide handelt bij Incident Response met de zorgvuldigheid die van een redelijk bekwaam en redelijk handelend vakgenoot mag worden verwacht, gegeven de beschikbare informatie en de urgentie van de situatie.

3.2 Beschikbaarheid en spoedinzet

3.2.1 Opdrachtgever erkent dat de beschikbaarheid van Securide voor acute Incident Response afhankelijk is van de op dat moment beschikbare capaciteit. Een 24/7-beschikbaarheid of gegarandeerde responstijd geldt uitsluitend indien dit schriftelijk is overeengekomen in een afzonderlijke Incident Response Retainer Agreement (IRRA).

3.2.2 Werkzaamheden buiten reguliere kantooruren, in weekenden of op feestdagen worden afzonderlijk in rekening gebracht tegen het bij Securide gebruikelijke overwerktarief, tenzij anders overeengekomen in een IRRA.

3.3 Aansprakelijkheid bij noodmaatregelen

3.3.1 Opdrachtgever erkent dat Incident Response wordt uitgevoerd in een crisisomgeving met beperkte informatie en tijdsdruk. Onverminderd artikel 5 van dit Addendum is Securide niet aansprakelijk voor schade die voortvloeit uit:

(a) maatregelen genomen op instructie of met goedkeuring van Opdrachtgever;

(b) maatregelen die redelijkerwijs noodzakelijk waren om verdere schade te beperken;

(c) het niet kunnen herstellen van versleutelde, beschadigde of verwijderde data die door een aanvaller is gewist of versleuteld;

(d) vertragingen veroorzaakt doordat Opdrachtgever de benodigde toegang, inloggegevens of medewerking niet tijdig beschikbaar stelt.

3.3.2 Opdrachtgever vrijwaart Securide voor aanspraken van derden die voortvloeien uit door Securide in het kader van Incident Response genomen maatregelen, mits Securide daarbij heeft gehandeld overeenkomstig de redelijkerwijs te verwachten professionele standaard.

3.4 Chain of custody en integriteit

3.4.1 Securide houdt bij Forensisch Onderzoek een gedocumenteerde Chain of Custody bij, waaruit blijkt (a) welke Forensische Data zijn vergaard, wanneer en door wie, (b) hoe de integriteit is geborgd, bijvoorbeeld door middel van hashwaarden, en (c) wie toegang heeft gehad tot de Forensische Data.

3.5 Bewaring, teruggave en vernietiging

3.5.1 Forensische Data worden uitsluitend verwerkt voor de in de opdrachtovereenkomst omschreven doeleinden en niet met derden gedeeld zonder uitdrukkelijke schriftelijke toestemming van Opdrachtgever, tenzij (i) een wettelijke verplichting daartoe bestaat, of (ii) medewerking wordt gevorderd door een opsporingsinstantie op grond van een rechtsgeldige vordering.

3.5.2 Na voltooiing van de opdracht worden forensische kopieen van data van Opdrachtgever binnen een door partijen te bepalen termijn vernietigd of geretourneerd, tenzij een wettelijke bewaarplicht van toepassing is.

3.6 Legal privilege

Indien Opdrachtgever aangeeft dat het forensisch rapport is bestemd voor gebruik in of ter voorbereiding op een juridische procedure, brengt Securide het rapport uitsluitend uit aan de advocaat van Opdrachtgever, tenzij schriftelijk anders is overeengekomen. Partijen maken in dat geval nadere afspraken over de vertrouwelijkheid en het gebruik van het rapport.

3.7 Medewerking aan opsporing en verzekeraars

3.7.1 Securide verleent op verzoek van Opdrachtgever, en voor zover dit redelijkerwijs van haar kan worden verlangd, medewerking aan (a) het verstrekken van informatie aan opsporingsinstanties op grond van een rechtsgeldige vordering en (b) het opstellen van verklaringen of rapportages ten behoeve van verzekeraarsclaims van Opdrachtgever. Hieruit voortvloeiend meerwerk wordt vergoed tegen het gebruikelijke uurtarief van Securide.

3.7.2 Securide is niet aansprakelijk voor schade die voortvloeit uit door haar te goeder trouw aan opsporingsinstanties of verzekeraars verstrekte informatie, voor zover zij daarbij naar beste weten en vermogen heeft gehandeld. Dit sluit aan op artikel 22.8 van de NLdigital Voorwaarden 2025.

Artikel 4 – Coordinated Vulnerability Disclosure en meldingen

4.1 Ontdekking van Kwetsbaarheden bij derden

4.1.1 Indien Securide bij de uitvoering van haar diensten Kwetsbaarheden ontdekt in systemen van derden die buiten de overeengekomen Scope vallen, zal Securide:

(a) Opdrachtgever onverwijld informeren over de aard en omvang van de bevinding;

(b) in overleg met Opdrachtgever bepalen of en hoe melding wordt gedaan bij de betrokken derde(n) en/of bij het NCSC, overeenkomstig de *Leidraad Coordinated Vulnerability Disclosure* van het NCSC;

(c) bij het melden handelen overeenkomstig de beginselen van proportionaliteit en subsidiariteit.

4.2 Ethische gedragscode

Securide handelt bij eigen meldingen van Kwetsbaarheden conform de *DIVD Code of Conduct* van het Dutch Institute for Vulnerability Disclosure en de CVD-leidraad van het NCSC. Deze kaders worden door het Openbaar Ministerie erkend als invulling van de beginselen voor niet-vervolging bij ethisch hacken. De volledige gedragscode van Securide is terug te vinden op de website van Securide.

4.3 Meldplichten NIS2 / Cyberbeveiligingswet en AVG

4.3.1 Indien Securide ontdekt dat sprake is of kan zijn van een Incident in de zin van de Cyberbeveiligingswet (de Nederlandse implementatie van de NIS2-richtlijn) of van een inbreuk in verband met persoonsgegevens in de zin van de AVG, stelt zij Opdrachtgever hiervan onverwijld, doch uiterlijk binnen acht (8) uur na ontdekking, op de hoogte.

4.3.2 De verantwoordelijkheid voor het beoordelen van de meldplicht en het verrichten van eventuele meldingen aan bevoegde autoriteiten (zoals het NCSC en de Autoriteit Persoonsgegevens) rust te allen tijde bij Opdrachtgever, in zijn hoedanigheid van verwerkingsverantwoordelijke of als entiteit die onder de Cyberbeveiligingswet valt.

4.3.3 Securide biedt op verzoek van Opdrachtgever ondersteuning bij het opstellen en indienen van meldingen, mits dit als afzonderlijke dienst is overeengekomen.

4.4 Geen aansprakelijkheid voor wettelijke meldingen

Opdrachtgever erkent dat Securide op grond van professionele ethiek en/of wettelijke verplichtingen gehouden kan zijn Kwetsbaarheden met significante maatschappelijke impact te melden bij het NCSC of andere bevoegde autoriteiten, ook zonder expliciete toestemming van Opdrachtgever, voor zover dit in overeenstemming is met de toepasselijke wet- en regelgeving. Securide is niet aansprakelijk voor schade die uit een dergelijke melding voortvloeit. Deze bepaling sluit aan op artikel 22.8 van de NLdigital Voorwaarden 2025.

Artikel 5 – Aansprakelijkheid en verzekering (security-specifiek)

5.1 Aansluiting bij artikel 15 NLdigital Voorwaarden 2025

5.1.1 Op de aansprakelijkheid van Securide is artikel 15 van de NLdigital Voorwaarden 2025 onverkort van toepassing. Dit betekent onder meer dat de aansprakelijkheid voor directe schade is beperkt tot de contractsom (bij een duurovereenkomst: de contractsom over een periode van één jaar), met een absoluut maximum van € 500.000, dat indirecte schade en gevolgschade zijn uitgesloten (artikel 15.4) en dat de aansprakelijkheidsbeperking niet geldt bij opzet of bewuste roekeloosheid van de bedrijfsleiding van Securide (artikel 15.6).

5.1.2 Rechtsvorderingen en verweren van Opdrachtgever in verband met de dienstverlening vervallen na verloop van vierentwintig (24) maanden, conform artikel 15.8 van de NLdigital Voorwaarden 2025.

5.1.3 De in dit artikel en in artikel 15 NLdigital genoemde beperkingen gelden gezamenlijk en niet cumulatief: de aansprakelijkheid van Securide overstijgt in geen geval de daarin opgenomen maxima.

5.2 Security-specifieke uitsluitingen

In aanvulling op artikel 15 NLdigital Voorwaarden 2025 geldt voor de security-dienstverlening van Securide het volgende:

(a) Securide is niet aansprakelijk voor schade als gevolg van cyberaanvallen, datalekken, ransomware of andere beveiligingsincidenten die zich voordoen na voltooiing van de overeengekomen diensten, ook indien door Securide geleverde diensten of adviezen in enige mate aan de beveiligingssituatie hebben bijgedragen;

(b) Securide is niet aansprakelijk voor schade die voortvloeit uit de omstandigheid dat door haar gemelde Kwetsbaarheden niet of niet tijdig door Opdrachtgever zijn verholpen;

(c) Securide is niet aansprakelijk voor schade die voortvloeit uit onjuiste of onvolledige informatie die Opdrachtgever heeft verstrekt over de te onderzoeken systemen of de eigendomsverhoudingen daarvan.

5.3 Koppeling aan beroepsaansprakelijkheidsverzekering

Securide houdt een adequate beroepsaansprakelijkheidsverzekering voor ICT-dienstverlening in stand. Op eerste verzoek van Opdrachtgever verstrekt Securide een bewijs van dekking. Voor zover een uitkering onder deze verzekering lager is dan de in artikel 5.1 genoemde maxima, is de aansprakelijkheid van Securide beperkt tot het door de verzekeraar daadwerkelijk uitgekeerde bedrag, vermeerderd met het toepasselijke eigen risico, behoudens in de gevallen genoemd in artikel 15.6 NLdigital Voorwaarden 2025.

5.4 Vrijwaring door Opdrachtgever

5.4.1 Opdrachtgever vrijwaart Securide voor alle aanspraken van derden, waaronder klanten van Opdrachtgever, eigenaren van testsystemen, toezichthouders en opsporingsinstanties, die voortvloeien uit:

(a) de uitvoering van diensten conform de overeengekomen Scope en opdracht;

(b) het handelen of nalaten van Opdrachtgever, waaronder het niet tijdig of onvolledig verhelpen van door Securide gemelde Kwetsbaarheden;

(c) door Opdrachtgever verstrekte onjuiste of onvolledige informatie over de te testen systemen of de eigendomsverhoudingen daarvan;

(d) bestuurlijke boetes die aan Opdrachtgever zijn opgelegd door een toezichthouder als gevolg van onvoldoende beveiliging.

5.4.2 Deze vrijwaring geldt niet voor zover de aanspraken aantoonbaar zijn veroorzaakt door opzet of bewuste roekeloosheid van de bedrijfsleiding van Securide.

5.5 Schriftelijke vastlegging van adviezen en geweigerde maatregelen

5.5.1 Securide legt door haar gegeven beveiligingsadviezen schriftelijk vast. Indien Opdrachtgever besluit een door Securide aanbevolen beveiligingsmaatregel niet of niet tijdig te implementeren, legt Securide deze beslissing schriftelijk vast en bevestigt zij dit aan Opdrachtgever. Voor schade die het gevolg is van het niet opvolgen van een aldus schriftelijk vastgelegd advies is Securide niet aansprakelijk.

Artikel 6 – Vertrouwelijkheid, rapportages en referenties

6.1 Vertrouwelijkheid van bevindingen

Alle bevindingen, rapportages, methoden en werkwijzen die Securide in het kader van haar security-dienstverlening opstelt of toepast, zijn strikt vertrouwelijk. Onverminderd de geheimhoudingsbepalingen van de NLdigital Voorwaarden 2025 worden security-rapportages uitsluitend gedeeld met de in de opdrachtovereenkomst aangewezen contactpersonen van Opdrachtgever.

6.2 Gebruik van rapportages door Opdrachtgever

Opdrachtgever deelt de door Securide gehanteerde werkwijze, methoden en rapportages niet met derden zonder voorafgaande schriftelijke toestemming van Securide, conform artikel 59.5 van de NLdigital Voorwaarden 2025. Dit geldt niet voor zover Opdrachtgever wettelijk verplicht is een rapportage te delen met een toezichthouder, auditor of opsporingsinstantie.

6.3 Verbod op gebruik voor AI-training

Conform artikel 7.2 van de NLdigital Voorwaarden 2025 is het partijen niet toegestaan gegevens, rapportages of resultaten van de andere partij te gebruiken voor het trainen van of het voeden van systemen voor kunstmatige intelligentie, behoudens voorafgaande schriftelijke toestemming.

6.4 Geanonimiseerde referenties

Securide is gerechtigd om in geanonimiseerde en niet tot Opdrachtgever herleidbare vorm gebruik te maken van opgedane kennis en ervaringen voor doeleinden van kennisontwikkeling, kwaliteitsverbetering en marketing. Securide vermeldt Opdrachtgever uitsluitend als referentie na diens voorafgaande schriftelijke toestemming.

Artikel 7 – Slotbepalingen

7.1 Verhouding tot de NLdigital Voorwaarden 2025

Dit Addendum is uitsluitend van toepassing in samenhang met de NLdigital Voorwaarden 2025 en maakt daarvan als vaste uitbreiding deel uit. Bepalingen van de NLdigital Voorwaarden 2025 die niet door dit Addendum worden gewijzigd, blijven onverkort van kracht. Bij strijdigheid prevaleert dit Addendum als de meer specifieke regeling. 7.2 Compliance-kader

Partijen erkennen dat op de dienstverlening, afhankelijk van de hoedanigheid van Opdrachtgever, aanvullende wettelijke kaders van toepassing kunnen zijn, waaronder de AVG, de Cyberbeveiligingswet (implementatie NIS2), de DORA-verordening en de Cyber Resilience Act. Hoofdstuk 2 (Compliance) van de NLdigital Voorwaarden 2025 is hierop van toepassing. Securide treedt bij de verwerking van persoonsgegevens op als verwerker; de verwerkersregeling in de artikelen 28 en volgende van de NLdigital Voorwaarden 2025 is van toepassing.

7.3 Wijzigingen

Securide is gerechtigd dit Addendum te wijzigen op gelijke wijze als waarop zij haar algemene voorwaarden wijzigt. De meest recente, door Securide gehanteerde versie van dit Addendum is van toepassing op haar aanbiedingen en dienstverlening.

7.4 Conversie

Indien een bepaling van dit Addendum nietig is of wordt vernietigd, blijven de overige bepalingen onverkort van kracht. De nietige of vernietigde bepaling wordt vervangen door een geldige bepaling die zoveel mogelijk aansluit bij de strekking van de oorspronkelijke bepaling.

7.5 Toepasselijk recht en geschillen

Op dit Addendum en op alle dienstverlening waarop het van toepassing is, is uitsluitend Nederlands recht van toepassing. Geschillen worden beslecht overeenkomstig de geschillenregeling in artikel 18 van de NLdigital Voorwaarden 2025, waaronder arbitrage door de Stichting Geschillenoplossing Automatisering (SGOA) te Amsterdam, behoudens geschillen die tot de bevoegdheid van de kantonrechter behoren.