

WinSys B.V.

MASTER SERVICE LEVEL AGREEMENT 2026

LiveBEDRIJF | Managed services | Cloud | Datacenter | Werkplek | Netwerk | Security | VoIP | AI

Kenmerk	Invulling
Versie	1.5 - definitief met visuals
Datum	18 september 2026
Dienstverlener	WinSys B.V., KvK 34100113, Westerduinweg 3, 1976 BV IJmuiden
Toepassing	Generiek voor alle zakelijke klanten en alle schriftelijk overeengekomen WinSys-diensten
Samenhang	Offerte/opdrachtbevestiging, deze SLA, Verwerkersovereenkomst 2026 v2.1 en algemene voorwaarden
Status	Definitieve generieke overeenkomst zonder invulvelden

Leeswijzer

Deze SLA behoeft geen klantspecifieke invulling. De concrete diensten, aantallen, prijzen en afwijkingen blijken uitsluitend uit de offerte, opdrachtbevestiging of een aantoonbare schriftelijke afspraak.

1. Partijen, doel, toepassing en rangorde

1.1 Partijen

Deze SLA geldt tussen WinSys B.V. (“WinSys”) en iedere zakelijke opdrachtgever (“Klant”) die met WinSys een hoofdovereenkomst, offerte of opdrachtbevestiging aangaat.

1.2 Scope

Alleen daadwerkelijk schriftelijk overeengekomen diensten vallen binnen scope. Voorbeelden of mogelijke opties in deze SLA scheppen zonder opdracht geen leveringsplicht.

1.3 Rangorde

Rang	Document	Primair onderwerp
1	Dwingend recht	Niet-afwijkbare verplichtingen
2	Verwerkersovereenkomst	Persoonsgegevens en artikel 28 AVG
3	Offerte of opdrachtbevestiging	Diensten, aantallen, prijzen en afwijkingen
4	Deze SLA	Generieke service-, security-, leveranciers- en exitafspraken
5	Algemene voorwaarden	Overige bepalingen

Technische productbeperkingen of leveranciersvoorwaarden beperken uitsluitend de betreffende derde-dienst en wijzigen niet de aansprakelijkheidsgrens, contractduur, opzegregeling, privacy- of exitverplichtingen van WinSys, tenzij dwingend recht of een uitdrukkelijke schriftelijke afspraak anders bepaalt.

2. Definities

Begrip	Betekenis
LiveBEDRIJF	De modulair afgenomen managed dienstverlening van WinSys.
Technisch beheer	Beschikbaar maken, beveiligen, monitoren, onderhouden en herstellen binnen scope.
Functioneel beheer	Beleid, processen, inhoud, rollen, bewaartermijnen en gebruik; standaard bij Klant.
P1	Volledige of vrijwel volledige uitval van een kritieke dienst zonder redelijke uitwijk, of een actief ernstig security-incident.
P2	Ernstige verstoring met grote impact en beperkte uitwijk.
P3	Reguliere storing of vraag met beperkte impact.
P4	Wijziging, advies, levering of project.
RTO	Doeltermijn voor dienstherstel.
RPO	Maximaal beoogd gegevensverlies in tijd.

Begrip	Betekenis
Security-incident	Gebeurtenis die beschikbaarheid, integriteit, vertrouwelijkheid of authenticiteit kan raken.
Co-sourcing	Gedeeld technisch beheer door WinSys en Klant of diens derde.

3. Dienstcatalogus en afbakening

Domein	Mogelijke onderdelen	Afbakening
Managed werkplek	Windows, M365 Apps, Intune, Autopilot, Endpoint, remote beheer	Binnen licentie en ondersteunde assets
Microsoft 365	Exchange, Teams, SharePoint, OneDrive, Entra, Defender, Purview	Leveranciersfunctionaliteit en tenantinstellingen
Azure/cloud	VM's, netwerk, identity, security, monitoring	Verbruik en architectuur volgens opdracht
Datacenter/private cloud	VM/VHD, opslag, netwerk, firewall, VPN, monitoring	Product, locatie en capaciteit volgens opdracht
Netwerk	Router, firewall, switches, wifi, VLAN, VPN	Alleen geregistreerde beheerde apparatuur
Servicedesk	Incident, verzoek, change, escalatie	Volgens servicevenster
Security	Identity/endpoint, alerts, awareness, rapportage, incidentrespons	Geen absolute preventiegarantie
Back-up/herstel	Serverversiegeschiedenis tot maximaal circa 90 dagen; aanvullende M365-, VM-, immutable/offsite- en restoreopties	Standaard serverherstel volgens hoofdstuk 9; uitbreiding alleen schriftelijk
VoIP	Nummers, configuratie, beheer en support	Providerafhankelijk
Web/applicatie	Plesk, SQL, Linux/Windows, koppelingen	Functionele inhoud bij Klant/leverancier
AI/Copilot	Technische governance, security, adoptie en awareness	Klant bepaalt rechtmatig functioneel gebruik
Hardware/projecten	Levering, installatie, migratie, training en consultancy	Offerte en planning

Datacenter- en hostingdiensten kunnen worden aangeboden onder LiveHOSTING of TrueHosting. VoIP kan worden uitgevoerd met A1 Internet/LiveVOIP. WinSys blijft centraal aanspreekpunt voor door WinSys gecontracteerde onderdelen.

3.1 Technische randvoorwaarden

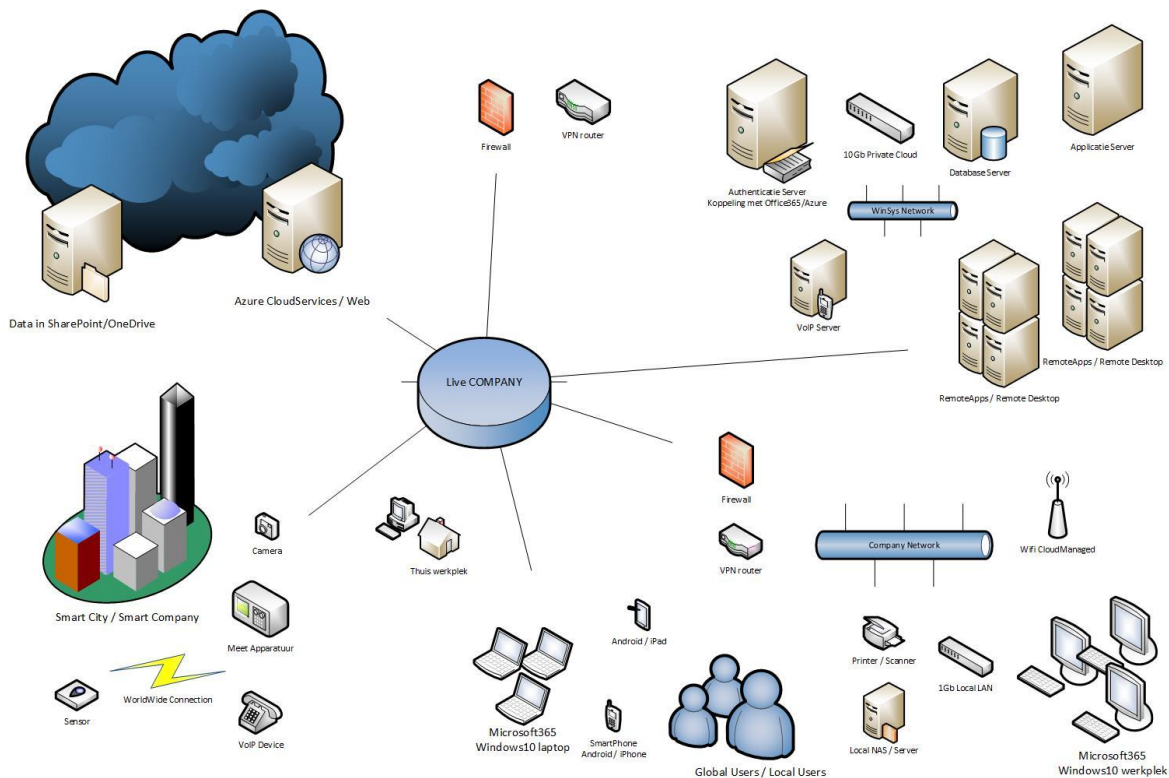
- Zakelijke internetverbinding: generiek minimaal 50 Mbit/s download en 20 Mbit/s upload per locatie, tenzij inventarisatie zwaardere capaciteit vereist.
- Intern bekabeld netwerk van minimaal 1 Gbit/s; 4G/5G kan optionele uitwijk zijn.
- Ondersteunde, geregistreerde apparatuur en actuele ondersteunde besturingssystemen.
- Geldige Microsoft-, CAL-, applicatie- en overige licenties.
- Noodzakelijke technische DNS- en domeinrechten voor overeengekomen beheer; juridisch domeinhouderschap blijft bij Klant.

3.2 Open-source, Linux, Seafile en webhosting

WinSys kan open-source en Linux-gebaseerde diensten leveren en technisch beheren, waaronder Linux-hosting, webhosting, containers, databases en samenwerkings- of bestandsplatformen zoals Seafile. Deze diensten kunnen afhankelijk van beschikbaarheid, capaciteit, security-eisen, datalocatie en continuïteitsontwerp worden gehost op WinSys-infrastructuur in IJmuiden, op dedicated door WinSys beheerde infrastructuur bij Hetzner of in een hybride combinatie van beide locaties.

Voor open-source software geldt dat WinSys verantwoordelijk is voor de overeengekomen technische installatie, hardening, updates, monitoring, back-up en beschikbaarstelling. Functionaliteit, community releases, upstream patches, compatibiliteit en supportduur zijn mede afhankelijk van het betreffende project of de leverancier. Maatwerk, plug-ins, datamigratie, functioneel beheer en ondersteuning buiten de overeengekomen scope zijn meerwerk.

Bij Plesk, Seafile, Linux-webhosting of vergelijkbare diensten wordt schriftelijk bepaald welke data, back-up, retentie, RPO, RTO, beheerrechten en locatie onderdeel van de dienst zijn. Een self-service back-upfunctie of versiegeschiedenis vervangt geen afzonderlijk overeengekomen WinSys-back-upvoorziening.



Figuur 2. Voorbeeld van lokale netwerksegmentatie en beheerde verbindingen binnen LiveBEDRIJF.

4. Verantwoordelijkheden en co-sourcing

Onderwerp	WinSys	Klant
Risico en beleid	Technisch advies en implementatie binnen scope	Risicobereidheid, beleid en wettelijke toepasselijkheid
Autorisatie	Technische uitvoering op aantoonbare instructie	Bevoegdheden, functiescheiding en goedkeuring

Onderwerp	WinSys	Klant
Applicaties derden	Best-effort technische beschikbaarstelling	Contract, licentie, inhoud en functionele support
Continuïteit	Overeengekomen back-up, herstel en test	Kritieke processen, RTO/RPO en acceptatie
Lokale omgeving	Beheerde geregistreerde componenten	Stroom, fysieke beveiliging en onbeheerde assets
Compliance	Technische informatie en medewerking	Registratie, bestuurstoezicht, formele meldingen en DPIA

4.1 Co-sourcing

Technische handelingen van Klant of derden worden gelogd waar technisch mogelijk. Klant draagt het risico van onbevoegde of niet-afgestemde wijzigingen. Indien Klant noodzakelijke toegang blokkeert, worden getroffen garanties en SLA-klokken opgeschort zolang WinSys redelijkerwijs niet kan beheren. Herstel vindt met verhoogde prioriteit plaats op nacalculatie, tenzij het incident aan WinSys toerekenbaar is.

5. Contactlijnen, servicedesk en servicelevels

5.1 Contactlijnen

Doel	Kanaal
Tickets, vragen, storingen, aanvragen	support@winsys.eu en servicedesk@winsys.eu
Helpdesk en kantoor	+31 255 540333
P1 escalatie 24x7	+31 6 19914115
P1 escalatie, tevens SMS	+31 6 49390576
P1 escalatie, tevens WhatsApp	+31 6 47018265
Bestuurlijke escalatie	directie@winsys.nl en +31 255 540333

P1 wordt naast ticketregistratie direct telefonisch gemeld. Sociale media en @serverloos zijn uitsluitend voor algemene mededelingen en geen geldig kanaal voor incidenten, privacyverzoeken of calamiteiten.

5.2 Servicevenster en prioriteit

Prioriteit	Reactie	Streeftijd herstel/workaround	Updates
P1	30 minuten, 24x7 indien afgenomen	4 uur of zo spoedig redelijkerwijs mogelijk	Elke 60 minuten
P2	2 kantooruren	1 werkdag	Dagelijks
P3	8 kantooruren	2 werkdagen	Bij relevante wijziging
P4	2 werkdagen	Volgens planning/offerte	Volgens afspraak

Servicedesk: werkdagen 08:30-16:30 Nederlandse tijd. Wachten op Klant, toegang, besluit, derde leverancier of overmacht schort de SLA-klok op.

6. Beschikbaarheid, onderhoud en leveranciersketen

6.1 Beschikbaarheid

Een beschikbaarheidsgarantie geldt alleen voor een schriftelijk overeengekomen meetpunt, percentage, servicevenster en meetmethode. Anders geldt een professionele inspanningsverplichting. Gepland onderhoud, noodonderhoud, klant-/derdenwijzigingen, licentietekort, onbeheerde componenten, externe internet/stroom en overmacht zijn uitgesloten voor zover redelijk en causaal.

6.2 Leveranciers- en ketenbeheer

WinSys gebruikt zorgvuldig geselecteerde infrastructuur-, cloud-, software-, telecom-, security- en supportleveranciers, waaronder Hetzner Online GmbH, Microsoft, A1 Internet/LiveVOIP, servicemanagementleveranciers en securitypartners. Alleen feitelijk ingezette leveranciers maken deel uit van de klantketen. WinSys beoordeelt leveranciers risicogebaseerd op continuïteit, security, privacy, datalocatie, support en exit. Subverwerkerswijzigingen volgen de verwerkersovereenkomst.

6.3 WinSys-infrastructuur op locaties van WinSys en Hetzner

WinSys levert haar datacenter- en hostingdiensten met eigen technische oplossingen, eigen architectuur, eigen beheerprocessen en eigen beveiligingsconfiguraties. Wanneer apparatuur fysiek in een datacenter van Hetzner staat, blijft de toegepaste server-, virtualisatie-, netwerk-, monitoring-, back-up- en beheeroplossing een door WinSys ontworpen en beheerde WinSys-oplossing. Hetzner levert in dat geval primair de fysieke datacenterlocatie, stroomvoorziening, koeling, fysieke beveiliging, connectiviteit en/of onderliggende infrastructuur die feitelijk is afgenomen.

De dedicated serverhardware die WinSys voor LiveBEDRIJF, LiveHOSTING, TrueHosting of andere hosted diensten inzet, is eigendom van WinSys of staat exclusief en dedicated ter beschikking van WinSys. Deze hardware wordt niet aan Klant verkocht en wordt niet door Klant of een opvolgende dienstverlener overgenomen, tenzij WinSys dit afzonderlijk schriftelijk overeenkomt. WinSys richt de servers in en beheert, onderhoudt, patcht, monitort en herstelt de systemen volgens de overeengekomen scope. Klant verkrijgt rechten op de overeengekomen diensten en klantdata, maar geen eigendoms- of beheerrechten op de fysieke WinSys-hosts.

WinSys houdt de logische klantomgevingen gescheiden. Virtuele machines, virtuele disks, containers, databases, applicaties en klantdata worden per klant of dienst logisch geïsoleerd en door WinSys beheerd. De fysieke locatie bij Hetzner verandert niet dat WinSys voor Klant het centrale aanspreekpunt en de technische beheerpartij blijft.



Figuur 1. LiveBEDRIJF: centrale WinSys-regie over werkplek, Microsoft-cloud, private cloud en netwerk.

WinSys kiest voor klantomgevingen standaard een EU/EER-locatie. Afhankelijk van de dienst kan hosting plaatsvinden op WinSys-infrastructuur in IJmuiden of op WinSys-infrastructuur en dedicated systemen in een Hetzner-datacenter, waaronder waar beschikbaar Falkenstein, Nürnberg of Helsinki. De feitelijke locatie, productvorm en eventuele aanvullende uitwijk of replicatie volgen uit de technische inrichting van de dienst. Een locatie buiten de EU/EER wordt alleen gebruikt na schriftelijke opdracht en met passende privacywaarborgen.

Voor zover Hetzner persoonsgegevens verwerkt of toegang kan hebben als gevolg van de afgenomen datacenter- of infrastructuurdienst, zorgt WinSys dat passende artikel 28 AVG-afspraken in de verwerkersketen gelden. De WinSys-verwerkersovereenkomst blijft leidend tussen Klant en WinSys.

6.4 Hetzner Cloud SLA en credits

Voor Hetzner Cloud Servers en vServers vermeldt de leveranciers-SLA een maandelijkse beschikbaarheidsdoelstelling van 99,9% per instance, per kalendermaand. Het meetpunt betreft onderliggende host, hypervisor en instance-activiteit en is niet gelijk aan end-to-end beschikbaarheid van een applicatie of LiveBEDRIJF.

Leveranciersuitsluitingen kunnen onder meer zien op klantconfiguratie, klantsoftware, rescaling, noodzakelijke live-migratie, bepaalde aanvallen/malware, externe netwerkproblemen en overmacht. Hetzner-compensatie is Cloud Credit voor toekomstig gebruik. Een credit is geen schadevergoeding, verhoogt de WinSys-aansprakelijkheidsgrens niet en wordt alleen verwerkt indien feitelijk ontvangen, de klantdienst is geraakt en de schriftelijke opdracht daarin voorziet.

6.5 Dedicated WinSys-beheer, leveranciersproducten, back-up en kosten

Hetzner kan bepaalde Cloud Servers of dedicated producten op leveranciersniveau als unmanaged aanbieden. Dit doet geen afbreuk aan de overeengekomen managed dienstverlening van WinSys: wanneer een server of dienst door WinSys als onderdeel van LiveBEDRIJF wordt geleverd, voert WinSys het overeengekomen technische beheer uit. Een server, snapshot, volume of leveranciersback-upoptie vormt niet automatisch een volledige beheerde back-upgarantie. Alleen de door WinSys overeengekomen inrichting, monitoring, back-up, retentie, RPO, RTO en restoretests vallen binnen de dienst. Resources kunnen kosten veroorzaken zolang zij bestaan, ook als zij zijn uitgeschakeld. Leverancierskosten mogen doorlopen totdat een resource volgens het exitplan veilig is gemigreerd, geëxporteerd of verwijderd. Voor de dedicated WinSys-hosts en daarop draaiende virtuele servers geldt daarnaast de standaard versiegeschiedenis en maximale herstelmogelijkheid uit hoofdstuk 9.

6.6 Overige leveranciers

Voor Microsoft 365, Azure, Entra ID, Teams, SharePoint, Exchange Online, OneDrive, Intune, Defender, Autopilot en Copilot gelden mede actuele Microsoft-product-, licentie- en servicevoorwaarden. Voor VoIP gelden mede provider- en porteringstermijnen. Voor securitytests gelden scope en geheimhouding van de securitypartner. Voor klantapplicaties gelden compatibiliteits- en supportvoorwaarden van de maker.

Leveranciers mogen producten, prijzen, voorwaarden, locaties en functies wijzigen. WinSys mag technisch gelijkwaardige wijzigingen uitvoeren wanneer nodig voor security, continuïteit, wetgeving of leverancierswijzigingen. Materiële gevolgen voor prijs, datalocatie, security of functionaliteit worden vooraf of bij urgentie zo spoedig mogelijk gemeld. WinSys blijft verantwoordelijk voor redelijke coördinatie, escalatie en herstel binnen scope.

7. Security, Cyberbeveiligingswet en rapportage

Domein	Maatregelen voor zover passend en overeengekomen
Risico	Assets, scope, risicoanalyse, changes en afhankelijkheden
Incident	Detectie, triage, containment, herstel, communicatie en evaluatie
Continuïteit	Back-up, restoretest, uitwijk en herstellprioriteiten
Keten	Leveranciers, subverwerkers en wijzigingen
Kwetsbaarheden	Patchen, hardening, scanning en optionele pentest
Identity	MFA, least privilege, privileged access en lifecycle
Encryptie	Transport en waar passend at rest
Effectiviteit	Monitoring, audit, rapportage en PDCA

Voor klanten onder de Cyberbeveiligingswet ondersteunt WinSys binnen scope bij technische maatregelen, risico-informatie en incidentinformatie. Klant blijft verantwoordelijk voor kwalificatie, registratie, bestuurlijke goedkeuring, bestuurstraining en formele meldingen.

7.1 Incidentmelding

WinSys meldt een relevant security-incident of datalek zonder onredelijke vertraging en uiterlijk binnen 24 uur na ontdekking en voldoende vaststelling dat de klantomgeving of persoonsgegevens kunnen zijn geraakt. Een voorlopige melding wordt aangevuld zodra informatie beschikbaar is.

7.2 Certificeringen en rapportage

WinSys beschikt volgens de aangeleverde certificaten over ISO 9001:2015 FM 708610, ISO/IEC 27001:2022 IS 708611 en NEN 7510-1:2017+A1:2020 NEN 7510-081 binnen de gecertificeerde scope. Certificering van het managementsysteem is geen absolute product- of wettelijke garantie. Geautoriseerde klantrollen kunnen, voor zover licenties dit toelaten, toegang krijgen tot relevante Microsoft security- en compliance-informatie. Maatwerkrapportages en auditdossiers zijn meerwerk tenzij inbegrepen.

8. Privacy, subverwerkers en internationale doorgifte

De WinSys Verwerkersovereenkomst 2026 v2.1 regelt persoonsgegevens, instructies, geheimhouding, TOMs, subverwerkers, datalekken, rechten van betrokkenen, audits, doorgifte, AI, exit en verwijdering. Voor privacy prevaleert deze overeenkomst en dwingend recht. WinSys verwerkt klantdata niet voor eigen modeltraining zonder schriftelijke afspraak en geldige grondslag. Doorgifte buiten EER vindt uitsluitend plaats met een geldige AVG-grondslag en waarborgen.

9. Back-up, versiegeschiedenis, herstel en continuïteit

9.1 Standaard herstelvoorziening voor WinSys-servers

Voor de door WinSys beheerde Windows-serveromgevingen en virtuele servers maakt WinSys standaard gebruik van versiegeschiedenis op server- en virtuele-diskniveau, technisch uitgevoerd met beschikbare shadow-copy- of vergelijkbare snapshotfunctionaliteit. Deze standaardvoorziening geldt voor de virtuele servers die draaien op WinSys-infrastructuur in IJmuiden én voor virtuele servers die draaien op dedicated, door WinSys beheerde servers die fysiek bij Hetzner zijn geplaatst. De fysieke datacenterlocatie verandert de standaard WinSys-herstelmethodiek niet.

De versiegeschiedenis wordt waar technisch ondersteund op de relevante virtuele disk of geselecteerde volumes ingericht en stelt WinSys in staat bestanden en mappen terug te zetten naar een beschikbaar eerder herstelpunt. De standaard maximale herstelperiode is maximaal circa negentig dagen terug, voor zover de betreffende herstelpunten op dat moment nog technisch beschikbaar en leesbaar zijn. Oudere herstelpunten worden binnen de normale cyclus overschreven. Negentig dagen is daarmee de maximale standaard herstelmogelijkheid die WinSys op deze servers aanbiedt, en geen garantie dat voor iedere dag, ieder tijdstip of ieder bestand een afzonderlijk herstelpunt beschikbaar is.

9.2 Reikwijdte en technische beperkingen

Onderdeel	Standaardpositie
Omgeving	Door WinSys beheerde Windows-servers en virtuele servers in IJmuiden of op dedicated WinSys-infrastructuur bij Hetzner.
Methode	Versiegeschiedenis via shadow copy of technisch vergelijkbare snapshotfunctie op virtuele disk of geselecteerde volumes.
Maximale standaard herstelperiode	Maximaal circa 90 dagen terug, uitsluitend voor nog aanwezige en leesbare herstelpunten.
Overschrijven	Herstelpunten ouder dan de beschikbare cyclus worden automatisch overschreven.
Herstelniveau	Bestanden en mappen; volledige systeemrestore uitsluitend indien technisch mogelijk en afzonderlijk overeengekomen.
Niet standaard	Onafhankelijke offsite full backup, immutable kopie, archief, gegarandeerd dagelijks herstelpunt of onbeperkte historie.
Linux/open source	Alleen volgens de voor die dienst schriftelijk overeengekomen back-upmethode; Windows shadow copy is niet automatisch van toepassing.
Microsoft 365	Versie-, retentie- en herstelmogelijkheden volgen licentie, tenantconfiguratie en eventueel apart afgenomen WinSys-back-up.

Versiegeschiedenis bevindt zich technisch in of nabij hetzelfde server- of opslagdomein en is daarom geen volledige vervanging voor een onafhankelijke back-up. Een defecte of corrupte virtuele disk, ransomware, versleuteling, logische corruptie, foutieve replicatie, verwijdering of andere storing kan één of meer herstelpunten onbruikbaar maken. RAID, redundantie, replicatie, snapshots en versiegeschiedenis verhogen de herstelbaarheid, maar zijn afzonderlijk geen garantie tegen dataverlies.

9.3 Herstelverplichting en maximale standaardprestatie

WinSys spant zich bij een geldig herstelverzoek in om het meest geschikte nog beschikbare herstelpunt binnen de maximale standaardperiode van circa negentig dagen te selecteren en de gevraagde bestanden of mappen terug te plaatsen. De herstelprestatie is begrensd door de inhoud, integriteit en beschikbaarheid van het laatst bruikbare herstelpunt. WinSys kan niet meer gegevens herstellen dan in het beschikbare herstelpunt aanwezig zijn.

Herstel vindt plaats op aantoonbare instructie van een bevoegde contactpersoon. WinSys mag vooraf een veilige doelmap, geïsoleerde locatie of alternatieve bestandsnaam gebruiken om overschrijven van actuele data te beperken. Klant controleert na herstel de functionele juistheid, volledigheid en bruikbaarheid. Herstel als gevolg van een fout van Klant, een derde, co-sourcing of functioneel beheer wordt tegen het geldende tarief uitgevoerd, tenzij schriftelijk ingebrepen. Herstel dat noodzakelijk is door een aan WinSys toerekenbare technische fout binnen scope wordt volgens de overeenkomst behandeld.

9.4 Aanvullende back-upopties

Een ruimere of sterkere herstelvoorziening geldt alleen wanneer deze schriftelijk is overeengekomen. Mogelijke aanvullende opties zijn een periodieke volledige kopie van een virtuele disk, een kopie naar een andere WinSys-locatie,

Azure, een externe gegevensdrager of NAS, een offsite of immutable back-up, langere retentie, applicatiebewuste databaseback-up, extra herstellpunten en periodieke restoretests. De offerte of opdrachtbevestiging bepaalt databron, frequentie, retentie, locatie, encryptie, RPO, RTO, testfrequentie en kosten.

Een real-time kopie of synchronisatie naar een tweede server is geen zelfstandige back-up zolang fouten, verwijderingen of versleuteling kunnen worden meegesynchroniseerd. Een beoogde totale historie van bijvoorbeeld 180 dagen ontstaat alleen wanneer twee technisch onafhankelijke en afzonderlijk ingerichte herstelcycli daadwerkelijk zijn overeengekomen en operationeel zijn. Retentieperioden worden niet automatisch bij elkaar opgeteld.

9.5 Linux, Seafile, Plesk en open-source hosting

Voor Linux, Seafile, Plesk, containers, databases en overige open-source diensten wordt de back-up ingericht met een technisch passende methode. De standaard Windows-versiegeschiedenis van maximaal circa negentig dagen is daarop niet automatisch van toepassing. Zonder afzonderlijke schriftelijke back-upafpraak geldt uitsluitend de in de dienst aanwezige self-service-, snapshot- of versiefunctie, voor zover beschikbaar. Indien WinSys-back-up wordt afgenomen, worden bron, frequentie, retentie, locatie en herstelprocedure schriftelijk bepaald.

9.6 Microsoft 365, Teams, SharePoint en OneDrive

Microsoft 365-versiegeschiedenis, prullenbak, retentie en herstel worden bepaald door de actuele Microsoft-licentie, workload, tenantconfiguratie en het ingestelde beleid. Deze functies zijn niet automatisch gelijk aan de serverversiegeschiedenis van WinSys en vormen niet zonder afzonderlijke afspraak een onafhankelijke WinSys-back-up. Een aanvullende kopie naar een WinSys-virtuele server in IJmuiden of bij Hetzner geldt alleen wanneer deze dienst expliciet is afgenomen.

9.7 Monitoring, controle en continuïteit

WinSys bewaakt de overeengekomen server- en back-upcomponenten technisch en registreert relevante meldingen en herstelhandelingen. Monitoring bevestigt niet automatisch dat iedere individuele file dagelijks herstelbaar is. Een inhoudelijke steekproef of volledige restoretest vindt uitsluitend plaats volgens de overeengekomen testfrequentie. Voor kritieke systemen legt Klant de gewenste RPO en RTO vast; WinSys beoordeelt of de standaard versiegeschiedenis daarvoor voldoende is of dat aanvullende back-up en uitwijk nodig zijn.

9.8 Exit en verwijdering

Bij exit verstrekt WinSys redelijk beschikbare informatie over de laatste back-upstatus, de gebruikte herstelmethode en de resterende retentie. Versiegeschiedenis en back-ups blijven niet onbeperkt beschikbaar en worden na afloop van de dienst volgens de normale cyclus, de verwerkersovereenkomst en wettelijke bewaarplichten verwijderd of overschreven. Een speciale export, full backup of externe gegevensdrager wordt tegen het geldende tarief uitgevoerd, tenzij schriftelijk inbegrepen.

10. Changes, onboarding en offboarding

- Standaard change: vooraf goedgekeurd, laag risico en herhaalbaar.
- Normale change: impact, planning, akkoord en terugvalplan waar passend.
- Spoedchange: direct noodzakelijk voor incident, security of continuïteit; achteraf geregistreerd en geëvalueerd.

Onboarding gebeurt op aantoonbare instructie met minimale standaardrechten. Offboarding omvat blokkeren, sessies intrekken, MFA/middelen, licenties en instructie over mailbox/OneDrive/Teams. Zonder instructie gelden technische dienst- en licentievoorwaarden; overdracht van gebruikersdata vereist rechtmatige bevoegdheid.

11. Implementatie, migratie, fasering en acceptatie

11.1 Fase 0 - Inventarisatie en nulmeting

WinSys inventariseert de lokale, cloud- en serveromgeving, werkplekken, netwerk, internet, wifi, printers, scanners, IoT/randapparatuur, applicaties, databronnen, leveranciers, contracten, licenties, gebruikers, functies, rechten, beveiliging, back-up, continuïteit en bekende risico's. Klant stelt voldoende tijd, werkruimte, contactpersonen en noodzakelijke toegang beschikbaar. Tijdens deze fase wordt de productieomgeving niet zonder afzonderlijk akkoord gewijzigd.

Klant verstrekt waar van toepassing contactgegevens van functionele beheerders en applicatieleveranciers, een gebruikers- en rechtenoverzicht, licentiegegevens en beheerinformatie voor Microsoft 365, Azure, servers, NAS, netwerk, DNS en domeinen. Voor Microsoft 365/Azure kan tijdelijk Global Administrator-toegang of delegated admin via een partnerrelatie nodig zijn. Ontbrekende informatie wordt als risico, afhankelijkheid of restpunt in het Plan van Aanpak opgenomen.

Het resultaat van fase 0 is een overeengekomen scope, risico- en afhankelijkhedenoverzicht, doelarchitectuur op hoofdlijnen, migratievolgorde, verwachte hinder, benodigde licenties/hardware, verantwoordelijkheden en conceptplanning.

11.2 Fase 1 - Ontwerp, schaduwomgeving en Proof of Concept

WinSys bouwt waar passend een gescheiden test- of schaduwomgeving, virtualiseert onderdelen voor onderzoek, richt Microsoft 365/Teams/SharePoint, identity, policies, back-up en netwerkcomponenten technisch in en voert testmigraties uit. Testdata of een eerste kopie is niet per definitie actueel en wordt niet als productiebron gebruikt.

WinSys kan een Proof of Concept op een demonstratiewerkplek of laptop beschikbaar maken met de beoogde look-and-feel, Teams/SharePoint-indeling, policies, beveiliging en optioneel Copilot. Klant beoordeelt de functionele inrichting, rechten en bruikbaarheid. Pas na aantoonbaar akkoord op het Plan van Aanpak, de fasering en het go/no-go-besluit start de productiemigratie.

11.3 Fase 2 - Technische voorbereiding en productiemigratie

WinSys configureert de Common Operating Environment, werkplekken, Intune, Autopilot, endpointsecurity, applicaties, netwerken, VPN, printers en koppelingen voor zover in scope. Recente data wordt naar de doelomgeving overgezet of gesynchroniseerd. Voor maatwerksoftware werkt WinSys samen met de door Klant aangewezen leverancier; de functionele werking blijft bij Klant en leverancier.

De definitieve datamigratie en cutover kunnen tijdelijke onbeschikbaarheid veroorzaken. De planning vermeldt het onderhoudsvenster, de verwachte hinder, terugvaloptie, verantwoordelijkheden en communicatie. Mailmigraties, waaronder POP3/IMAP naar Microsoft 365, worden uitgevoerd met passende migratietooling; concrete garanties over downtime of volledigheid gelden alleen indien schriftelijk bevestigd na inventarisatie.

11.4 Fase 3 - Validatie, oplevering en overgang naar regulier beheer

Na de cutover valideert WinSys de technische werking, beveiliging, monitoring, back-up en beheerconnecties. Klant valideert gebruikers, rechten, applicatieprocessen en data-inhoud. Restpunten krijgen een eigenaar, prioriteit en planning. De migratie is technisch geaccepteerd wanneer de overeengekomen kernfuncties beschikbaar zijn en geen aantoonbare kritieke blokkade resteert.

WinSys draagt de projectdocumentatie intern over aan het beheerteam en schakelt de overeengekomen monitoring, servicedesk en escalatie in. Waar onderdeel van de opdracht wordt een gebruikerspresentatie of instructie gegeven. De in offerte of Plan van Aanpak genoemde productiedatum is de startdatum van regulier beheer en, tenzij schriftelijk anders bepaald, van de LiveBEDRIJF-contractperiode.

11.5 Projectgovernance en wijzigingen

De planning en besluitmomenten worden vastgelegd in het Plan van Aanpak. Afwijkingen in scope, aanvullende hardware, nieuwe applicaties, ontbrekende brondata, extra datavolume, leveranciersvertraging of nieuwe beveiligingseisen kunnen leiden tot een change, aangepaste planning of meerwerk. Akkoord kan schriftelijk of aantoonbaar digitaal worden gegeven.

12. Vergoeding, levering en opschorting

LiveBEDRIJF is standaard technisch beheer op vast maandtarief en functionele wijzigingen op nacalculatie, tenzij schriftelijk anders. Nieuwe gebruikers, werkplekken, uitbreidingen, applicaties, projecten en niet-operationeel onderzoek zijn meerwerk tenzij inbegrepen. Levertermijnen zijn indicatief tenzij uitdrukkelijk fataal overeengekomen.

Facturen zijn binnen 30 dagen verschuldigd. Opschorting na betalingsachterstand is proportioneel en volgt op ingebrekestelling en redelijke hersteltermijn, behalve bij fraude, misbruik of acute securitynoodzaak. Klantdata en wettelijk vereiste privacy- en exitmedewerking worden niet onbeperkt achtergehouden.

13. Aansprakelijkheid, garanties en overmacht

De totale gecumuleerde aansprakelijkheid van WinSys, uit welke hoofde dan ook en voor alle gebeurtenissen en aanspraken samen binnen één contractjaar, is beperkt tot maximaal de totale netto vergoeding exclusief btw voor twaalf maanden overeengekomen LiveBEDRIJF-diensten. Alleen terugkerende managed-servicemaandbedragen tellen mee; projecten, hardware, derdenlicenties, cloud-/telecomverbruik, reis- en doorbelaste kosten niet. Bij een kortere looptijd geldt twaalf maal het actuele maandbedrag. Geen verzekeringsuitkering, garantie, servicecredit of leverancierscredit verhoogt deze grens. De beperking geldt niet waar dwingend recht beperking verbiedt, waaronder opzet of bewuste roekeloosheid van de bedrijfsleiding.

Indirecte schade, gevolgschade, gederfde winst, gemiste besparingen en goodwillverlies zijn uitgesloten voor zover wettelijk toegestaan. Cyberincidenten zijn niet automatisch overmacht; oorzaak en redelijke beheersbaarheid zijn bepalend.

14. Looptijd, verlenging, opzegging en exit

14.1 Jaarovereenkomst

De overeenkomst heeft een initiële vaste looptijd van twaalf maanden en wordt na iedere periode automatisch en stilzwijgend met een nieuwe vaste periode van twaalf maanden verlengd, tenzij tijdig rechtsgeldig opgezegd. Voor afzonderlijk afgenomen LiveVOIP kan de offerte of opdrachtbevestiging uitdrukkelijk een maandelijks verlengbare en maandelijks opzegbare looptijd bepalen; in dat geval geldt die specifieke regeling uitsluitend voor LiveVOIP.

14.2 Opzegging en betaling

Klant kan ieder moment schriftelijk opzeggen met één maand opzegtermijn. De actieve dienstverlening eindigt daarna, maar de resterende maandtermijnen van de lopende twaalfmaandsperiode blijven volledig verschuldigd en mogen ineens worden gefactureerd. Niet-opzegbare, vooraf kenbare derdenverplichtingen blijven daarnaast verschuldigd. Opzegging uiterlijk één maand vóór de einddatum tegen die einddatum voorkomt een nieuwe jaarverlenging.

14.3 Ontbinding

Ontbinding wegens wezenlijke tekortkoming volgt na ingebrekestelling en redelijke hersteltermijn, tenzij nakoming blijvend onmogelijk is. Bij een aan WinSys toerekenbare wezenlijke tekortkoming zijn resterende termijnen niet zonder meer verschuldigd; dwingend recht en omstandigheden zijn leidend.

14.4 Exitproces

- WinSys registreert einddatum, contractperiode, financiële afrekening en transitiedatum.
- Klant wijst aantoonbaar een bevoegde transitiecontactpersoon en eventueel opvolgend beheerder aan.
- Partijen bepalen planning, afhankelijkheden, beveiligde kanalen en acceptatiemomenten.
- Fasen: inventarisatie, data/documentatie, beheerrechten, technische validatie, acceptatie en intrekking WinSys-toegang.

14.5 Overdracht

- Klantdata in overdraagbaar formaat binnen technische mogelijkheden.
- Minimaal één werkend, gevalideerd Microsoft 365 Global Administrator-account waarop Klant herstelgegevens en MFA zelfstandig beheert.
- Benodigde Exchange-, SharePoint-, Teams-, Intune- en privileged rollen.
- Entra-groepen, rollen, Conditional Access, enterprise apps en SSO-afhankelijkheden.

- Exchange-connectoren, transportregels, DKIM, DMARC en SPF.
- Teams, SharePoint, OneDrive, retentie en rechteninformatie.
- Intune, Autopilot, complianceprofielen, apps en gecontroleerde device release.
- Azure subscriptions, resources, rollen en klantgebonden secrets.
- DNS, domeinen, certificaten, netwerk/VLAN/VPN/firewallinformatie en klantapparatuur.
- Back-upstatus, databronnen, retentie en herstelprocedure.
- VoIP-nummers en providerprocedure; assetdocumentatie en open risico's/changes.

14.6 Beveiliging, IP en afronding

Secrets worden via gescheiden geverifieerde kanalen overgedragen. WinSys draagt geen eigen persoonsgebonden accounts, interne wachtwoorden, generieke scripts, broncode, templates, multi-tenanttools of interne securityarchitectuur over. WinSys mag eigen automatisering ontkoppelen zonder klantdata te verwijderen of beheer onnodig te blokkeren. Na validatie trekt WinSys eigen en gedelegeerde rechten in. Klant meldt concrete blokkades binnen zeven kalenderdagen; daarna geldt technische acceptatie als essentials bereikbaar zijn.

14.7 Exitkosten en leveranciers

Administratieve beëindiging en intrekken van WinSys-toegang zijn inbegrepen. Export, conversie, migratie, projectleiding, buiten-vensterwerk, media, dataverkeer, backuprestore en opvolgersondersteuning zijn tegen uurtarief of offerte. Leveranciersdoorlooptijden, portering, exportbeperkingen en resterende termijnen blijven gelden. Persoonsgegevens worden geretourneerd/verwijderd volgens de verwerkersovereenkomst en back-upcyclus. Fysieke dedicated servers, hosts, netwerkapparatuur en overige datacenterhardware die eigendom zijn van WinSys worden niet overgedragen. WinSys draagt wel de klantdata, overeengekomen exports, noodzakelijke beheerrollen en redelijk beschikbare klantdocumentatie over volgens artikel 14.5.

15. Sectoren en AI

15.1 Onderwijs

Waar overeengekomen worden Normenkader IBP, autorisatie, leerling-/medewerkerdata, ketenkoppelingen en auditondersteuning toegepast. Het bestuur blijft verantwoordelijk voor beleid en grondslag.

15.2 Zorg

Waar overeengekomen worden NEN 7510, logging, segmentatie, toegang, herstel en zorgkoppelingen uitgewerkt. WinSys-certificering geldt uitsluitend binnen de certificaatscope.

15.3 DORA

Voor financiële entiteiten kan een DORA-afspraken nodig zijn met functieomschrijving, datalocatie, prestatiedoelen, incidentbijstand, audit/toezichthouder, onderuitbesteding, testen, continuïteit en exit. Specifieke DORA-verplichtingen prevaleren waar toepasselijk.

15.4 AI en Copilot

WinSys ondersteunt technische security, rechten, classificatie, DLP en logging binnen licenties. Klant blijft verantwoordelijk voor rechtmatig gebruik, transparantie, menselijke controle en besluiten. Klantdata wordt niet voor eigen modeltraining gebruikt zonder schriftelijke afspraak en geldige grondslag.

Bijlage A - Generieke RACI

Activiteit	WinSys	Klant	Derde
------------	--------	-------	-------

Activiteit	WinSys	Klant	Derde
Nieuwe gebruiker	R	A	
Rechtenwijziging	R	A/C	
Patching beheerd	R/A	I	C
Functionele applicatiewijziging	C	A/R	R
Securityincident	R	A voor wettelijke melding	C
Restore	R	A voor instructie/acceptatie	
Leverancierswijziging	R	C/bezwaar conform DPA	R
Exit/export	R	A	C

R = uitvoerend; A = eindverantwoordelijk; C = geraadpleegd; I = geïnformeerd.

Bijlage B - Bronnen en normenkader

- Aangeleverde documenten: LiveBEDRIJF SLA-dienstbeschrijving 2025-2026, migratie-uitleg, LiveBEDRIJF-whitepaper, samenvatting/prijsopgave en LiveVOIP Zakelijk.
- Cyberbeveiligingswet, in werking sinds 15 augustus 2026.
- AVG, Verordening (EU) 2016/679, artikelen 28 en 32.
- DORA, Verordening (EU) 2022/2554.
- WinSys Verwerkersovereenkomst 2026 v2.1.
- WinSys-certificaten ISO 9001:2015 FM 708610, ISO/IEC 27001:2022 IS 708611 en NEN 7510-1:2017+A1:2020 NEN 7510-081.
- Hetzner Docs, Service Level Agreement for Cloud servers, Cloud and vServer Service Agreement, Data Protection at Hetzner, DPA en Cloud locations; geraadpleegd 18 september 2026.