Service Level Agreement

1do Managed IT

Versie: 2.6
Status: Definitief
Documentclassificatie: Vertrouwelijk

1. Versiebeheer

Versie	Datum	Samenvatting wijziging
2.5	15-9-2025	- Tekstueel aangepast ISO 27001:2022 (voorheen :2017) - SLA vorm Basic is vervallen (5.2) - Alinea toegevoegd voor servers met linux besturingsssysteem (6.1) - Service Manager benoemt in escalatieoverzicht
2.6	01-06-2026	- Hoofdstuk Informatiebeveiligingsincidenten toegevoegd

2. Inleiding

Deze Service Level Agreement (SLA) geeft een overzicht van de wijze waarop 1do vormgeeft aan de dienstverlening zoals vastgelegd in de dienstverleningsovereenkomst. Deze SLA is bedoeld voor beide partijen: 1do en Opdrachtgever. Met Opdrachtgever bedoelen we de organisatie met wie de Dienstverleningsovereenkomst is gesloten.

Wat kan Opdrachtgever van 1do verwachten en wat verwacht 1do van Opdrachtgever? In deze SLA wordt antwoord gegeven op deze vragen.

Het document is niet bedoeld 100% dekkend te zijn omdat wij van mening zijn dat, juist in de dienstverlening, flexibiliteit van doorslaggevend belang is voor een succesvolle samenwerking. Wel is het doel om bindende afspraken te maken over de kwaliteits-parameters van de dienstverlening en de rapportage hierover. Daar waar situaties ontstaan die niet gedekt worden binnen de SLA zullen aanvullende afspraken worden gemaakt.

Partijen kunnen in overleg de inhoud van de SLA wijzigen als deze van negatieve invloed is gebleken op de dienstverlening.

2.1 Algemene Voorwaarden

Op de SLA en het verlenen van de dienst zijn de Algemene Voorwaarden van 1do van toepassing. Opdrachtgever verklaart dat deze Algemene Voorwaarden bij of voorafgaand aan het sluiten van de overeenkomst ter beschikking zijn gesteld en akkoord gaat met de toepasselijkheid daarvan.

2.2 Dossier Afspraken en Procedures (DAP)

Het Dossier Afspraken en Procedures (hierna te noemen DAP) is een set van gemaakte operationele afspraken, die specifiek zijn vastgelegd voor Opdrachtgever. Het DAP is indien van toepassing als bijlage toegevoegd bij de dienstverleningsovereenkomst. Het DAP is in het documentatiesysteem voor alle 1do technici inzichtelijk en daarnaast bijgevoegd als bijlage bij deze SLA.

2.3 Geldigheidsduur

De start- en einddatum van de SLA (en van de eventuele DAP in bijlage) is gelijk aan de bovenliggende dienstverleningsovereenkomst. De onderhavige SLA vervangt eerder gemaakte mondelinge of schriftelijke afspraken.

3. Bereikbaarheid

Voor het afhandelen van vragen en incidenten biedt 1do ondersteuning vanuit het 1do Supportcenter. Voor vragen omtrent planning en inzetbaarheid van 1do medewerkers wordt ondersteuning gegeven door het 1do Projectbureau.

Vragen kunnen kenbaar gemaakt worden via e-mail, het 1do Serviceportaal of via de telefoon. We maken in principe geen onderscheid welke medewerkers van Opdrachtgever het Supportcenter mogen benaderen met vragen.

De voorkeur van 1do is dat bij Opdrachtgever intern bekend is welke medewerkers geautoriseerd zijn om contact met 1do op te nemen. Desgewenst kan Opdrachtgever bepalen dat dit slechts is voorbehouden aan bepaalde personen. Indien van toepassing wordt dit vastgelegd in een DAP.

3.1 Algemene contactgegevens

Wanneer	Onderdeel	E-mail	Telefoon
Reguliere werkdagen 8.00 - 17.00 uur	Supportcenter	supportcenter@1do.nl	+31 (0)88 - 444 50 50
	Projectbureau	projectbureau@1do.nl	+31 (0)88 - 444 50 70
	Sales	sales@1do.nl	+31 (0)88 - 444 50 40
Buiten kantooruren	Supportcenter Calamiteitendienst	supportcenter@1do.nl	Nummer wordt verstrekt bij afname van deze extra dienst

Reguliere werkdagen zijn van maandag tot en met vrijdag van 8.00 uur tot 17.00 uur.

Op nationale feestdagen is het Supportcenter niet geopend. Een aantal dagen per jaar is het Supportcenter vanaf 16.00 uur gesloten. Dit zijn Goede Vrijdag en 5, 24 en 31 december wanneer deze op een werkdag vallen.

3.2 Calamiteitendienst

Voor acute, bedrijfskritische verstoringen, buiten openingstijden van het Supportcenter stelt 1do een telefonische calamiteitendienst ter beschikking. Voor de bereikbaarheid van deze calamiteitendienst worden afspraken-op-maat gemaakt met Opdrachtgever. Uitgangspunt van deze dienst is dat de bereikbaarheid wordt uitgebreid naar beschikbaarheid op werkdagen van 7.00 tot 23.00 uur.

De calamiteitendienst is een aanvullende dienst bovenop deze standaard SLA en kent daarom een aanvullende tariefstelling. Voor toegang tot deze aanvullende dienst geldt er een maandelijkse toeslag. Daarnaast wordt per incident / oproep de daadwerkelijk door ons bestede tijd in rekening gebracht met een minimum van één uur. Uurtarieven en toeslagen zoals vermeld in de Dienstverleningsovereenkomst.

Het speciale telefoonnummer wordt (bij afname van deze dienst) uitsluitend beschikbaar gesteld aan door Opdrachtgever aangewezen contactpersonen.

4. Afspraken samenwerking

4.1 Rolverdeling

Als Opdrachtgever en 1do werken we met elkaar samen aan een veilige en betrouwbare IT-omgeving. Helder vastleggen wie welke verantwoordelijkheden heeft en welke werkzaamheden uitvoert, vinden we belangrijk voor een goede samenwerking en dit geeft duidelijkheid voor alle betrokkenen. Ook eventueel andere betrokken leveranciers kunnen in de rolverdeling worden opgenomen.

De rolverdeling is vastgelegd in een DAP.

4.2 Mandaat

Binnen de vastgestelde rolverdeling werken we samen en zorgen we over en weer voor de nodige afstemming en terugkoppeling. Er kunnen situaties optreden waarbij (snelle) voortgang noodzakelijk is. Het vooraf afstemmen en goedkeuring krijgen van de Opdrachtgever kan het proces dan ongewenst vertragen. Vanuit de rolverdeling en de verantwoordelijkheden die we daarin hebben werkt 1do vanuit het mandaat om in dergelijke situaties werkzaamheden zonder afstemming vooraf uit te voeren. Door dit specifieke mandaat werkt dat vaak efficiënter in tijd en kosten. Deze mandaatafspraak wordt vastgelegd in de scope van de Dienstverleningsovereenkomst.

Voorbeelden van dergelijke situaties kunnen zijn een gepubliceerde kwetsbaarheid waarvoor een hotfix is verschenen die snel moet worden geïnstalleerd. Of een belangrijke aanpassing in de Microsoft cloud die moet worden opgevolgd om beveiliging of correcte werking te blijven garanderen.

Voor de opvolging van informatiebeveiligingsincidenten geldt een apart mandaat, die is uitgewerkt in paragraaf 8.4 Mandaat tot direct ingrijpen.

5. SLA indeling

5.1 SLA vormen

De Managed IT dienstverlening is beschikbaar in diverse SLA pakketten. Een pakket bepaalt waar de SLA op van toepassing is. Dat is mogelijk op losse onderdelen, namelijk 'Server', 'Werkplek' of 'Netwerkapparatuur'. Daarnaast is er een All-in-1 pakket waarbij alle SLA-diensten zijn samengebracht in één pakket.

Een SLA pakket bestaat uit een aantal onderliggende diensten die zijn onderverdeeld in de SLA-types Standard en Plus. Afhankelijk van het SLA-type valt de dienst ofwel in de abonnementskosten ofwel worden hiervoor aanvullende kosten gerekend.

De SLA-vorm die voor Opdrachtgever van toepassing is, is vastgelegd in de Dienstverlenings-overeenkomst. Indien geen afgenomen SLA-vorm staat vermeld, dan is geen SLA van toepassing.

5.2 Onderdelen per SLA vorm

In onderstaande tabel is per pakket en SLA-type weergegeven welke onderliggende onderdelen daar binnen vallen.

	Server / Werkplek		Netwerk		All-in-1
SLA-onderdeel	**Standard**	**Plus**	**Standard**	**Plus**	**Premium**
Automatische monitoring	✓	✓	✓	✓	✓
Monitoring van back-ups	✓	✓	✓	✓	✓
Updatebeheer	✓	✓	€	€	✓
Ondersteuning door 1do supportcenter & opvolging alerts	€	✓	€	✓	✓
Restore van gebruikersbestanden	€	✓			✓
Periodieke server controles (APK)	€	✓			✓
Smartphones/tablets ondersteuning	€	€			✓
Microsoft Cloudbeheer	€	€			Optie

✓ : Valt binnen de SLA.
€ : Worden aanvullende kosten voor berekend.

5.3 Onderdelen All-in-1 pakket

De dienstverlening binnen het All-in-1 pakket zijn onderverdeeld in een aantal hoofdcategorieën.
In de Dienstverleningsovereenkomst is vastgelegd welke diensten specifiek met Opdrachtgever zijn overeengekomen.

De hoofdcategorieën van het All-in-1 pakket zijn:

1 - Microsoft Cloudbeheer
2 - Servers en Apparatuur
3 - Werkplekbeheer
4 - Gebruikersondersteuning

6. Toelichting diensten

6.1 Toelichten bepaalde diensten

Van een aantal diensten geven we graag wat meer inzicht in wat dit omvat.

Microsoft Cloudbeheer
Servers, opslagsystemen, werkplekken en netwerkapparatuur moeten worden onderhouden en beheerd, een Microsoft cloudomgeving moet dat ook. Voor sommige zaken gebeurt dat op Organisatie-/tenant-niveau, andere zaken concentreren zich maar op applicaties, logging, gebruikers- of device-zaken. Stilstand is achteruitgang en dat geldt zeker ook voor een cloudomgeving. De Microsoft cloud (365 en Azure) worden operationeel en beschikbaar gehouden door Microsoft, de inrichting en beveiliging is aan de gebruiker ervan (de Organisatie dus). 1do neemt binnen deze overeenkomst de rol van beheerder op zich. Het kan zijn dat uit deze monitoring en bewaking verbetersuggesties voortvloeien die projectmatig moeten worden benaderd. In dergelijke gevallen zal 1do adviseren.

Voor sommige zaken geldt dat deze pas gemonitord en beheerd kunnen worden als er ook licenties voor aanwezig zijn en zaken voor ingericht zijn. Denk bijv. aan het bewaken van ingerichte email-domeinbeveiliging: dit kan alleen plaatsvinden als hiervoor de noodzakelijke inrichting heeft plaatsgevonden en als (de licenties voor) monitoring aanwezig zijn. In het algemeen geldt: hoe meer input, hoe meer bewaking. 1do zal hierover adviseren.

Servers en Apparatuur
Het is hiervoor bij het cloudbeheer al gezegd: ook servers, opslagsystemen, werkplekken en netwerkapparatuur moeten worden onderhouden en beheerd. Voor al deze systemen geldt de monitoring en het updatebeheer zoals hierna nader omschreven, maar daarnaast ook zaken als het bewaken van logboeken, opvolgen alarmen uit monitoring, herstarten van servers en services, bewaken back-ups incl. proefrestores, snapshot-beheer, opruim- en opschoonacties etc. Voor servers en werkplekken geldt dat ook security-zaken zoals antivirus software en firewalls moeten worden bewaakt.

Het beheer, onderhoud en ondersteuning van servers met een *Linux besturingssysteem* valt buiten deze SLA en is uitdrukkelijk de verantwoordelijkheid van Opdrachtgever. Dergelijke servers worden wél in basis opgenomen in de monitoring voor het controleren van de up/down-status en indien technisch mogelijk ook monitoring op capaciteit (Geheugen, Processor, Schijfruimte). Eventuele aanvullende of afwijkende afspraken kunnen worden vastgelegd in een DAP.

Werkplekbeheer
Binnen werkplekbeheer ondersteunen we medewerkers van Opdrachtgever met de apparatuur rondom de werkplek. Daarin helpen we met vragen en problemen rondom gebruikersaccounts, laptops en pc's. Hiervoor richten we ook de monitoring en het updatebeheer in zoals hierna nader omschreven, als ook security-zaken zoals bewaken van antivirus software. We leveren uiteraard ook ondersteuning op smartphones en tablets. Bij het All-in-1 pakket is dit inbegrepen; bij de andere pakketten wordt dit buiten de SLA opgepakt.

Automatische monitoring
Signalering ofwel monitoring is de basis van onze invulling van IT-beheer. Monitoring geeft 1do de "ogen en oren" in de IT-omgeving van Opdrachtgever. Monitoring, maar vooral ook de opvolging ervan, is daarom cruciaal in ons proces. Binnen 1do houden naast geautomatiseerde systemen een aantal medewerkers de systemen van onze opdrachtgevers nauwlettend in de gaten houden. 1do maakt hiervoor gebruik van diverse gespecialiseerde monitoring software. Er is een uitgebalanceerde template opgesteld die van toepassing is op de betreffende IT-systemen. Waar nodig wordt voor Opdrachtgever een maatwerktemplate opgesteld die als onderdeel van de DAP dan wordt vastgelegd.

Updatebeheer
1do zorgt door middel van updatebeheer voor het periodiek bijwerken van (beveiligings)updates van het Microsoft Windows besturingssysteem en bepaalde basisapplicaties: Microsoft Office, Microsoft Exchange Server en Microsoft SQL Server. Daarnaast kan een aantal veelgebruikte kantoorapplicaties ook periodiek worden bijgewerkt, denk aan veelgebruikte internetbrowsers zoals Google Chrome en Mozilla Firefox en bijvoorbeeld PDF-readers.

Voor sommige updates kan extra toezicht nodig zijn op de installatie. Denk aan Servicepacks op de server-besturingssystemen of updates die door een fabrikant worden uitgebracht wanneer kwetsbaarheden of beveiligingslekken in software zijn ontdekt die met prioriteit moeten worden bijgewerkt. Updates waarvoor dit extra toezicht nodig is worden vanzelfsprekend wel uitgevoerd, maar vallen buiten de scope van het reguliere updatebeheer.

Naast updates van Windows Servers, werkplekken en basisapplicaties, moet ook andere (netwerk)apparatuur van tijd tot tijd worden bijgewerkt. Voor apparatuur die in de overeenkomst is opgenomen verzorgen wij ook hier het updatebeheer. Opgemerkt moet worden dat met name bij netwerkapparatuur, waarbij vaak een volledige IT-omgeving van de beschikbaarheid van deze apparatuur afhankelijk is, bij het plaatsen van beschikbare updates een afweging wordt gemaakt van de toegevoegde waarde van zo'n update. Kritische- en beveiligingsupdates worden vanzelfsprekend wel altijd geïnstalleerd.

Bij cloudomgevingen is in zekere zin ook sprake van "updatebeheer" als het gaat om het inrichten of gebruik maken van nieuwe voorzieningen, functionaliteiten, (beveiligings)instellingen. Dit is binnen deze overeenkomst afgedekt binnen het cloudbeheer.

Back-up & Restore
Als binnen de IT-omgeving van Opdrachtgever back-ups worden gemaakt, zorgt 1do dat de logging hiervan dagelijks wordt bewaakt. Op verzoek ondersteunen we bij een restore. Desgewenst kunnen we afspraken maken (vastgelegd in een DAP) dat 1do periodiek een test-restore uitvoert, waarvan Opdrachtgever dan ook terugkoppeling ontvangt. Als een restore nodig is in het kader van Disaster Recovery, valt dit buiten de SLA, maar ondersteunen we om dit spoedig en doeltreffend te laten verlopen.

Server-APK
Servers met een SLA-type Managed IT Plus of All-in-1 worden door 1do periodiek nagelopen conform vaste checklists. Het doel hiervan is om tijdig en proactief te kunnen reageren op verstoringen of afwijkingen.

6.2 Werkzaamheden binnen Managed IT All-in-1 Premium

Op basis van de afgesproken verantwoordelijkheden voor 1do (in de scope van de Overeenkomst) worden de benodigde werkzaamheden uitgevoerd en berekent 1do hoeveel tijd binnen het All-in-1 pakket beschikbaar wordt gesteld. Bij de Service Review wordt Opdrachtgever geïnformeerd of de huidige SLA te laag, toereikend of misschien zelfs te hoog is ingezet. Per half jaar kan dit bijgesteld worden als hier aanleiding voor is, wat daarmee ook van invloed op de hoogte van het maandbedrag.

6.3 Werkzaamheden binnen Managed IT PLUS

Binnen een PLUS-abonnement zijn kosten voor bepaalde SLA-werkzaamheden inbegrepen in het maandbedrag. Binnen deze Managed IT Plus-contracten voor servers en werkplekken worden vanuit het Supportcenter de volgende werkzaamheden uitgevoerd:

- Oplossen van incidenten;
- Beantwoorden van servicevragen;
- Incidentele restore van gebruikersbestanden uit back-ups;
- Opvolgen van meldingen uit automatische monitoring;
- Basis gebruikersbeheer (toevoegen/verwijderen inlogaccounts);
- Kleine aanpassingen: Fair use.

6.4 Werkzaamheden buiten SLA

Bepaalde werkzaamheden zullen altijd buiten de overeenkomst worden afgehandeld tegen het geldende uurtarief. Het betreft werkzaamheden op het gebied van:

- Werkzaamheden aan bedrijfsapplicaties (zoals financiële, ERP of CRM-software);
- Hardware- of softwarematige uitbreidingen of upgrades, zoals vervanging werkplekken en printers of vervanging van softwareprogramma's;
- Werkzaamheden naar aanleiding van informatiebeveiligingsincidenten of cybercriminaliteit (zoals phishing, cryptolocker-, malware- of virusuitbraak); de werkwijze voor respons en initiële opvolging gelden de afspraken zoals opgenomen in hoofdstuk 8: Informatiebeveiligingsincidenten;
- Uitvoering van werkzaamheden voor disaster recovery;
- Werkzaamheden die uitsluitend op klantlocatie uitvoerbaar zijn;
- Problemen in thuisnetwerken of privé apparatuur van medewerkers;
- Handmatige installatie van firmwares en kritische updates;
- Opvolgen van adhoc kwetsbaarheden met meer dan 2 uur arbeid;
- Incidenten die ontstaan ten gevolge van het negeren van een advies tot aanpassing.

7. Ondersteuning Supportcenter

7.1 Aanspreekpunt

Binnen 1do wordt samengewerkt vanuit verschillende disciplines/expertises. Voor Opdrachtgever streven we zoveel mogelijk naar het toewijzen van een vaste engineer of consultant. Deze medewerker kent de ins en outs van Opdrachtgever en komt op locatie voor werkzaamheden. Voor de reguliere ondersteuning bieden we ondersteuning met supportmedewerkers en beheerders. De supportmedewerkers zijn voor alle supportvragen het eerste aanspreekpunt.

7.2 Meekijken op afstand

In voorkomende gevallen kan een medewerker van 1do op afstand meekijken op het beeldscherm van een medewerker van Opdrachtgever. De medewerker van 1do zal niet ongevraagd meekijken. 1do maakt voor deze voorziening hoofdzakelijk gebruik van de speciale monitoringsoftware die 1do hiervoor op de werkplekken van Opdrachtgever heeft geïnstalleerd. Eventuele aanvullende afspraken kunnen worden vastgelegd in een DAP.

7.3 Serviceportaal

Via het 1do Serviceportaal (https://serviceportaal.1do.nl/) is het voor Opdrachtgever mogelijk om meldingen te maken. Voordeel van het Serviceportaal is dat er direct meer informatie wordt verzameld en de melding daarmee sneller op de juiste plek komt. In het Serviceportaal is de voortgang van een melding in te zien en kan waar nodig aanvullende informatie worden doorgegeven. Desgewenst kan een vast contactpersoon van Opdrachtgever toegang krijgen tot alle tickets van Opdrachtgever.

7.4 Documentatie

1do zorgt voor het vastleggen van alle relevante documentatie van de IT-omgeving van Opdrachtgever. Documentatie bestaat o.a. uit (installatie)beschrijvingen, procedures, wachtwoorden, foto's en IT-schema's. Alle werkzaamheden en bestede tijd wordt vastgelegd in het ticketsysteem.

7.5 Notificaties & statusupdates

Van meldingen in ons ticketsysteem worden statusupdates verstuurd. Bij het aanmaken en afsluiten van meldingen in het ticketsysteem ontvangt de melder een statusupdate per mail. Desgewenst is het mogelijk om ook deze statusmails ook naar een vast contactpersoon van Opdrachtgever te sturen. Indien van toepassing wordt dit vastgelegd in een DAP en ingericht in het ticketsysteem.

7.6 Meldingstypes

Binnenkomende meldingen worden onderverdeeld in vier meldingstypes:
1) Incident - 2) Servicevraag - 3) Aanpassing - 4) Informatiebeveiligingsincident

De afspraken rond informatiebeveiligingsincidenten zijn uitgewerkt in hoofdstuk 8 van deze SLA.

7.7 Afhandeling Aanpassing

Met een melding van het type aanpassing wordt bedoeld uitbreidingen, vernieuwingen of veranderingen aan de bestaande configuratie. Bij een aanpassing wordt in principe geen vaste prioriteit toegekend. De afhandeling hiervan gaat in goed onderling overleg. Uiteraard streven we ernaar deze melding tijdig en doeltreffend af te handelen. Waar mogelijk vragen we Opdrachtgever gewenste aanpassingen tijdig door te geven.

Het doorvoeren van een aanpassing door het Supportcenter wordt in principe niet binnen het contract gedekt. Kleine aanpassingen worden o.b.v. fair-use doorgevoerd. In de periodieke Service Review (zie hoofdstuk 10) wordt afgestemd of het aantal en omvang van kleine aanpassingen passend zijn binnen het contract en de overeengekomen prijsstelling.

7.8 Afhandeling Servicevraag

Een servicevraag is een algemene vraag, met een verzoek om informatie of een advies. Bij een servicevraag wordt in principe geen vaste prioriteit toegekend. De afhandeling hiervan gaat in goed onderling overleg. Uiteraard streven we ernaar deze melding tijdig en doeltreffend af te handelen.

7.9 Afhandeling Incidenten

Er is sprake van een incident wanneer een proces of functionaliteit niet werkt zoals het zou moeten (en voorheen wel probleemloos functioneerde). Incidenten worden door 1do in basis opgepakt op volgorde van binnenkomst, waarbij de indeling op prioriteit een rol speelt bij de opvolging.

Voor het vaststellen van de prioriteit maakt 1do gebruik van onderstaande matrix. Daarbij wordt een afweging gemaakt op basis van impact en urgentie. Waar nodig wordt voor bepaling prioriteit met Opdrachtgever overlegd.

Prioriteit = Impact x Urgentie

Impact	
1	meerdere afdelingen / hele organisatie kan niet werken
2	één afdeling kan niet werken of ondervindt andere hinder
3	één medewerker ondervindt hinder

Urgentie	
A	workaround is niet beschikbaar, oplossing kan niet worden uitgesteld
B	workaround is beschikbaar, maar oplossing kan niet worden uitgesteld
C	workaround is beschikbaar, oplossing kan worden uitgesteld

Prioriteit		Impact		
		1	2	3
Urgentie	A	Kritisch	Ernstig	Standaard
	B	Ernstig	Standaard	Laag
	C	Standaard	Laag	Laag

Aanmelding en response

Voor het aanmelden van een incident geeft 1do per prioriteitsniveau richting voor de voorkeurswijze van aanmelding. Daarnaast hanteren we uitgangspunten voor responsetijden.

Prioriteit	Aanmelding via	Aanvang werkzaamheden
Kritisch	Telefoon	Binnen 0,5 uur
Prio1 – Ernstig	Telefoon, Serviceportaal, mail	Binnen 1 uur
Prio2 – Standaard	Serviceportaal, mail of telefoon	Best effort, streven 1 dag
Prio3 - Laag	Serviceportaal, mail	Geen afspraak

7.10 Afhankelijkheid derden

Voor het leveren van continuïteit op producten of diensten bij Opdrachtgever kan sprake zijn van afhankelijkheid van de dienstverlening van toeleveranciers. Bijvoorbeeld een situatie met een defect aan een server waarop een servicecontract bij de fabrikant is afgesloten. Of een incident in een softwarepakket waar de helpdesk van de fabrikant nodig is. De snelheid en beschikbaarheid van toeleveranciers is van invloed op de voortgang van de afhandeling door 1do. Als betreffende toeleveranciers niet presteren zoals verwacht, is 1do in dergelijke gevallen daarvan afhankelijk en zal in overleg gezocht moeten worden naar een passende oplossing. Eventuele bijkomende kosten zijn daarbij voor rekening van Opdrachtgever.

1do biedt alleen ondersteuning op producten waarvoor ook vanuit de fabrikant ondersteuning mogelijk is. Daarbij kan 1do niet garanderen dat support op verouderde producten nog leverbaar is en zal dergelijke aanvragen op best-effort basis behandelen.

8. Informatiebeveiligingsincidenten

8.1 Definitie

Een informatiebeveiligingsincident is een gebeurtenis of reeks van samenhangende gebeurtenissen waarbij de vertrouwelijkheid, integriteit of beschikbaarheid van informatie, accounts, gegevens of IT-systemen van Opdrachtgever mogelijk of daadwerkelijk is aangetast.

Dit hoofdstuk beschrijft de wijze waarop 1do opvolging geeft aan meldingen van informatie-beveiligingsincidenten bij Opdrachtgever. 1do wordt betrokken deze meldingen om de dreiging te identificeren, in te perken, te elimineren of de omgeving weer beheersbaar te laten functioneren.

Voorbeelden van informatiebeveiligingsincidenten zijn:

- phishingincidenten;
- ransomware- of malwarebesmettingen;
- (vermoedens van) ongeoorloofde toegang tot accounts, systemen of data;
- lekken van vertrouwelijke informatie of persoonsgegevens;
- vernietiging, versleuteling of manipulatie van gegevens;
- misbruik van accounts, mailboxen, apparatuur.

8.2 Melden van informatiebeveiligingsincident

Een (vermoed) informatiebeveiligingsincident dient door Opdrachtgever altijd telefonisch te worden gemeld bij het Supportcenter van 1do.

Opdrachtgever verstrekt bij de melding voor zover mogelijk direct de relevante context en omvang van het incident, zoals:

- aard van het incident of vermoeden daarvan (phishingmail, ransomware, etc.);
- betrokken gebruiker, account, werkplek, server, netwerkonderdeel;
- reeds bekende impact of aanwijzingen voor bijv. ongeoorloofde toegang of verspreiding;
- door Opdrachtgever reeds genomen maatregelen of uitgevoerde handelingen.

8.3 Respons door 1do

Na binnenkomst van de melding start 1do binnen 1 uur (Prio 1) met eerste onderzoek en de initiële opvolging gericht op het identificeren en inperken van het informatiebeveiligingsincident.

Voor werkzaamheden ten aanzien van herstel en evaluatie geldt geen vaste doorlooptijd. De duur hiervan is afhankelijk van aard, omvang, complexiteit en afhankelijkheden van het incident.

1do zal zich inspannen om, voor zover redelijkerwijs mogelijk, rekening te houden met het behoud van relevante sporen en beschikbare log- of systeeminformatie die van belang kan zijn voor nadere analyse of onderzoek, voor zover dit het inperken, stoppen of herstellen van het informatiebeveiligingsincident niet belemmert.

8.4 Mandaat tot direct ingrijpen

Indien de aard of ernst van het informatiebeveiligingsincident daarom vraagt, heeft 1do het mandaat om zonder voorafgaande afstemming tijdelijke of directe beheersmaatregelen te nemen die redelijkerwijs nodig zijn om verdere schade, verspreiding of ongeoorloofde toegang te beperken of te stoppen.

Dergelijke maatregelen kunnen onder meer bestaan uit het blokkeren van accounts, het beëindigen van sessies, het isoleren van systemen of werkplekken, het uitschakelen van koppelingen, het intrekken van toegangsrechten of andere maatregelen die naar het oordeel van 1do noodzakelijk zijn voor het inperken van het incident.

8.5 Afwaarderen of herclassificeren

Indien uit de eerste beoordeling blijkt dat geen sprake is van een informatiebeveiligingsincident, is 1do gerechtigd de melding af te waarderen of te herclassificeren naar een regulier incident, servicevraag of aanpassing.

8.6 Afronding incidentfase
Een informatiebeveiligingsincident geldt als afgerond zodra naar het oordeel van 1do de acute dreiging is weggenomen en de betrokken omgeving weer beheersbaar functioneert.

Werkzaamheden die daarna nodig zijn voor structurele verbetering, herinrichting, hardening, aanvullende maatregelen of andere vervolgacties worden beschouwd als vervolgwerkzaamheden en kunnen projectmatig of als aanvullende werkzaamheden worden opgepakt.

8.7 Rolverdeling en medewerking Opdrachtgever
Opdrachtgever blijft verantwoordelijk voor:

- het intern signaleren en escaleren van mogelijke informatiebeveiligingsincidenten;
- het beschikbaar hebben van eigen interne contact- en escalatiestructuren;
- het tijdig en volledig aanleveren van relevante informatie;
- het tijdig nemen van benodigde besluiten aan klantzijde;
- het verlenen van medewerking die redelijkerwijs nodig is voor adequate opvolging.

Vertraging, onvolledigheid of het uitblijven van informatie, medewerking of besluitvorming aan de zijde van Opdrachtgever kan van invloed zijn op de snelheid en effectiviteit van de opvolging door 1do.

Specifieke klantafspraken over contactpersonen voor privacy en informatiebeveiliging, bereikbaarheid, escalatie en eventuele bijzondere meldafspraken kunnen worden vastgelegd in het DAP.

8.8 Privacy en meldplichten
Indien een informatiebeveiligingsincident tevens een datalek of mogelijk datalek betreft, blijft Opdrachtgever verantwoordelijk voor de beoordeling en eventuele melding aan toezichthouders, betrokkenen, sectorale instanties, verzekeraars of andere derden, tenzij wet- of regelgeving anders bepaalt.

1do verstrekt aan Opdrachtgever de informatie waarover zij beschikt, zodat Opdrachtgever aan zijn eventuele meldplichten kan voldoen, een en ander in aanvulling op de toepasselijke bepalingen uit de Algemene Voorwaarden.

8.9 Werkzaamheden en doorbelasting
De werkzaamheden die voortvloeien uit een informatiebeveiligingsincident worden afgehandeld tegen het geldende uurtarief en vallen niet binnen de reguliere SLA-dekking, tenzij schriftelijk anders is overeengekomen.

8.10 Rapportage en evaluatie
Een formele rapportage of nadere evaluatie wordt niet standaard bij ieder incident opgeleverd. Indien Opdrachtgever daarom verzoekt, of indien 1do dit gezien aard en omvang van het incident wenselijk acht, kunnen nadere rapportage, evaluatie of advieswerkzaamheden aanvullend worden uitgevoerd tegen het geldende uurtarief.

9. Aanvullende werkzaamheden

Naast werkzaamheden die binnen deze SLA worden uitgevoerd, kan 1do aanvullende werkzaamheden uitvoeren die ook van invloed zijn op de Dienstverleningsovereenkomst, SLA en DAP.

9.1 Beheer op afspraak

Periodiek kan met een medewerker van 1do een afspraak op locatie worden gemaakt. In dat bezoek worden allerlei werkzaamheden opgepakt, die bijvoorbeeld zijn opgespaard in de voorliggende periode. Dat kunnen uitbreidingen of aanpassingen zijn, maar ook het oplossen van knelpunten of het optimaliseren van de systemen. Ook voeren wij tijdens zo'n bezoek werkzaamheden uit die met het daadwerkelijke beheer en onderhoud van de IT-omgeving te maken hebben (met mogelijk ook opvolging van zaken die uit monitoring of controles naar boven komen).

Uit ervaring blijkt dat zo'n bezoek ook een goede gelegenheid is om vragen te stellen of om eventuele toekomstige aanpassingen te bespreken. Face to face communiceert toch nog altijd het makkelijkst. De bezoekfrequentie stellen we uiteraard samen vast, doorbelasting van de werkzaamheden vindt plaats op basis van de daadwerkelijk bestede tijd.

In de Dienstverleningsovereenkomst worden eventuele afspraken vastgelegd over de frequentie, aard en locatie van deze bezoekafspraken.

9.2 Gepland onderhoud

IT-Systemen vragen van tijd tot tijd onderhoud waardoor deze tijdelijk niet beschikbaar zijn. In principe worden alle voorkomende werkzaamheden uitgevoerd binnen reguliere kantoortijden. Er kunnen zich situaties voordoen dat dit niet passend is. In die gevallen kunnen de werkzaamheden in onderlinge afstemming ook buiten kantoortijden worden uitgevoerd. De bestede tijd zal in die gevallen worden doorbelast tegen het van toepassing zijnde uurtarief.

In het DAP zijn (indien van toepassing) afspraken vastgelegd over vaste onderhoudstijden. Denk aan kantoortijden waarop IT-Systemen beschikbaar moeten zijn en onderhoud niet gewenst is.

9.3 Projecten

Voor grotere uitbreidingen, vernieuwingen of aanpassingen aan de IT-omgeving zal vooraf de nodige afstemming plaatsvinden tussen Opdrachtgever en 1do. Na afloop van een project vindt ook een evaluatie van de Dienstverleningsovereenkomst plaats om te zorgen dat deze waar nodig wordt aangepast op de veranderde omgeving.

10. Verantwoordelijkheden Opdrachtgever

Naast de inzet van 1do, vraagt het optimaal invullen van de dienstverlening ook een stuk betrokkenheid van Opdrachtgever. Hierin leggen we daarom in alle redelijkheid bij Opdrachtgever een aantal verantwoordelijkheden:

- Opdrachtgever zorgt ervoor dat relevante medewerkers op de hoogte zijn van de afspraken in deze SLA.

- Opdrachtgever zet zich in om 1do naar beste vermogen te informeren en waar mogelijk te assisteren bij het afhandelen van een melding. Minimale informatie bij meldingen bestaat uit:
    - Bedrijfsnaam van Opdrachtgever;
    - Naam van de contactpersoon voor deze melding bij Opdrachtgever;
    - Contactgegevens ((mobiel) telefoonnummer en/of e-mailadres) van die contactpersoon;
    - Beschrijving van de Aanpassing, Servicevraag of het Incident, zo accuraat als mogelijk;
    - Beschrijving van de door Opdrachtgever reeds genomen stappen;
    - Omschrijving van de impact of omvang van het Incident.

- Opdrachtgever zorgt voor interne communicatie van relevante informatie aan (nieuwe) medewerkers van Opdrachtgever. Praktijk leert dat voldoende instructie en overdracht over de gebruikte IT-systemen bijdraagt aan sneller optimaal gebruik maken van de systemen.

- Opdrachtgever is verantwoordelijk voor de instructie van medewerkers op het gebied van databeveiliging als preventie om ongeoorloofd gebruik van de IT-systemen tegen te gaan. Denk bijvoorbeeld aan hoe om te gaan met phishing.

- Wanneer het installeren van bepaalde updates op hard- en software alleen mogelijk is als bij de desbetreffende fabrikant ook een servicecontract is afgesloten, zorgt Opdrachtgever ervoor dat deze contracten zijn afgesloten. Uiteraard geeft 1do hierin de nodige adviezen. Denk aan een Cisco Smartnet die daarmee toegang verschaft tot relevante software voor op de apparatuur. Zonder Smartnet is deze software niet beschikbaar.

- Opdrachtgever zorgt zelf dat haar eigen medewerkers beseffen dat aanpassingen/uitbreidingen die worden gevraagd aan 1do, voor additionele kosten kunnen zorgen.

- Opdrachtgever zorgt dat 1do (tijdig) wordt geïnformeerd bij veranderingen in de organisatie die van invloed kunnen zijn op de IT-omgeving.

- Opdrachtgever verstrekt aan 1do de contactinformatie van eventuele toeleveranciers. Deze gegevens worden opgeslagen in de documentatie bij 1do. Eventuele specifieke afspraken met dergelijke partijen kunnen worden opgenomen in het DAP.

11. Privacy en beveiliging

Informatiebeveiliging is een belangrijk thema in onze dienstverlening. Niet in de laatste plaats vanwege onze certificering op ISO 27001:2022. In onze bedrijfsvoering werken we vanuit deze richtlijn.

Vanwege de aard van de dienstverlening heeft 1do (in)direct toegang tot informatiesystemen en gegevens van Opdrachtgever. De werkzaamheden in het kader van deze dienstverleningsovereenkomst zijn daardoor per definitie vertrouwelijk.

Algemene aandachtspunten voor 1do:
- 1do neemt noodzakelijke maatregelen om de vertrouwelijkheid en integriteit van informatiesystemen en gegevens van Opdrachtgever te waarborgen.
- 1do zal niet zonder schriftelijke toestemming van Opdrachtgever enig detail omtrent de organisatie en medewerkers, processen, producten, systemen of activiteiten van Opdrachtgever delen met andere partijen.
- 1do kan desgewenst van betrokken medewerkers voor Opdrachtgever een VOG aanleveren. Kosten hiervoor komen voor rekening van Opdrachtgever.
- 1do zal in overleg met Opdrachtgever na eventuele beëindiging van de Overeenkomst zorgen voor overdracht van de bij 1do in bezit zijnde documentatie.

Aandachtspunten op het gebied van uitvoering van werkzaamheden:
- Zowel Opdrachtgever en 1do delen onderling geen persoonsgegevens tenzij de situatie hierom vraagt.
- Opdrachtgever wordt er met klem op gewezen geen logingegevens door te geven per telefoon, e-mail of via servicetickets. Als deze gegevens nodig zijn, dan altijd gebruikersnaam los van een wachtwoord verstrekken. Wachtwoorden worden versleuteld doorgegeven.
- Autorisatieverzoeken van Opdrachtgever worden alleen opgepakt als deze schriftelijk worden ingediend of bevestigd door Opdrachtgever.

12. Service Review

Om onze dienstverlening te bespreken en waar nodig te verbeteren is regelmatig contact noodzakelijk. Dat doet 1do in de vorm van de periodieke service review. Streven is om jaarlijks minimaal twee Service Review gesprekken te houden.

Het doel is wat het woord zegt: review (beoordelen) van de invulling van het IT-beheer. Over en weer. Evalueren hoe de dienstverlening is geweest en ervaren, hoe de uitvoering van onze dienstverlening in de praktijk werkt en verbeterpunten benoemen. Feedback werkt twee kanten op: als 1do ziet dat bepaalde zaken aan kant van Opdrachtgever verbeterd kunnen worden om een betere gezamenlijke performance te halen, dan worden die tijdens de service review benoemd.

Bij het service review overleg is vanuit Opdrachtgever in elk geval de vaste contactpersoon aanwezig en vanuit 1do een verantwoordelijk aanspreekpunt ofwel accountmanager. Wanneer nodig kunnen ook andere personen aanschuiven bij dat overleg.

Partijen kunnen waar nodig aanvullende afspraken vastleggen in een DAP.
Agendapunten voor de Service Review kunnen zijn:

- Kwaliteit en afhandeling van incidenten;
- Kwaliteit van de communicatie op diverse niveaus;
- Kennisniveau van beheerders en gebruikers;
- Evaluatie van prioriteit-1 incidenten, wijze van aanpak en oplossingen;
- Doornemen van afgenomen periodieke producten en diensten (o.a. licenties);
- Bespreken van bestede tijd door 1do binnen de overeenkomst;
- Verbeterpunten en concrete acties.

13. Escalatie

In een SLA mag een paragraaf over escalatie niet ontbreken. Wat te doen als ondanks alle goede bedoelingen er toch niet wordt geleverd wat wel verwacht wordt of wat is afgesproken? In die gevallen moet kunnen worden geëscaleerd, zowel binnen 1do als aan de zijde van Opdrachtgever.

Binnen de dienstverlening van 1do streven we ernaar om de lijnen zo kort mogelijk te houden. Dat geldt daarmee ook voor eventuele escalatie. De procedure voorziet in contactoverleg volgens escalatie-treden (van boven naar onder) zoals weergegeven in onderstaande tabel:

Trede	**Niveau**	**Opdrachtgever**	**1do**
0	Support	Eindgebruikers	Supportcenter
1	Manager	IT Aanspreekpunt / management / directie	Service Manager Operationeel Manager
2	Directie	Directie / management / IT-aanspreekpunt	Directie

14. Ondertekening

Aldus overeengekomen, akkoord bevonden en digitaal ondertekend.