Bijlage 1b – Service Level Agreeement

Inhoudsopgave

1. Inleiding, doel en reikwijdte 3

2. Incidentenmanagement 4

2.1 Incidentclassificatie, responsetijden en oplostijden 4

2.2 Statusupdates en communicatie 4

2.3 Inspanningsverplichting bij externe incidenten 5

2.4 Definities per type incident en voorbeelden 5

3. Changemanagement 8

3.1 Changeclassificatie, doorlooptijden en goedkeuringsprocedures 8

3.2 Statusupdates en communicatie 8

3.3 Inspanningsverplichting bij externe changes 9

3.4 Change Management Proces 9

3.5 Best Practices en borging 9

3.6 Definities per type change en voorbeelden 10

4. Escalatiematrix en 24x7 Bereikbaarheid P1 13

1. Inleiding, doel en reikwijdte

Deze Service Level Agreement (SLA) beschrijft de afspraken tussen de VRFGV en de Leverancier met betrekking tot het registreren, prioriteren, opvolgen, oplossen van ICT-incidenten én het uitvoeren van wijzigingen (changes) binnen de ICT-dienstverlening. Het doel van deze SLA is om heldere verwachtingen te scheppen over de kwaliteit, snelheid en transparantie van zowel incidentafhandeling als changemanagement, zodat de continuïteit van de bedrijfsvoering optimaal wordt gewaarborgd en risico's op verstoringen of beveiligingsincidenten worden geminimaliseerd.

Deze SLA geldt voor alle geplande en ongeplande wijzigingen en incidenten met impact op de ICT-dienstverlening, waaronder software-updates, configuratiewijzigingen, nieuwe functionaliteiten, noodmaatregelen en incidenten die voortkomen uit of direct verband houden met de dienstverlening van de Leverancier. Storingen of beperkingen veroorzaakt door externe leveranciers of derde partijen (zoals Microsoft of andere serviceproviders) vallen buiten de reikwijdte van deze SLA. In dergelijke gevallen zal de Leverancier zich inspannen om de VRFGV te informeren en de voortgang te monitoren, maar kan geen garanties geven over de oplostijd of doorlooptijd.

Door duidelijke afspraken te maken over de afhandeling van incidenten en changes, wordt de betrouwbaarheid van de ICT-dienstverlening verhoogd en kunnen risico's tijdig worden gesignaleerd en gemitigeerd. Transparantie in communicatie en het vastleggen van verantwoordelijkheden zijn hierbij cruciaal. De samenwerking tussen beide partijen wordt hiermee versterkt, met als doel een stabiele, veilige en toekomstbestendige ICT-omgeving.

2. Incidentenmanagement

2.1 Incidentclassificatie, responsetijden en oplostijden

Incidenten worden geclassificeerd op basis van urgentie en impact. Voor elk incident geldt een maximale responsetijd en oplostijd, mits de oorzaak binnen de invloedssfeer van de Leverancier ligt.

Type incident	Definitie	Responsetijd	Oplostijd	Norm
Prio 1 (P1) – Kritisch	Kritieke incidenten met directe impact op bedrijfscontinuïteit, veiligheid of dienstverlening. Geen workaround mogelijk.	2 uur	4 uur	95% per maand binnen oplostijd
Prio 2 (P2) – Hoog	Belangrijke incidenten met impact op een afdeling, locatie of groep gebruikers. Werk deels mogelijk, soms workaround.	4 uur	8 uur	90% per maand binnen oplostijd
Prio 3 (P3) – Midden	Minder urgente incidenten met beperkte impact, individuele gebruikers of niet-kritische systemen. Werk kan doorgaan, workaround mogelijk.	8 uur	2 werkdagen	90% per maand binnen oplostijd
Prio 4 (P4) – Laag	Verzoeken en incidenten zonder directe impact op bedrijfsvoering, bijvoorbeeld cosmetische issues of niet-essentiële wijzigingen.	48 uur	5 werkdagen	85% per maand binnen oplostijd

2.2 Statusupdates en communicatie

Bij incidenten met prioriteit P1 en P2 krijgt de VRFGV via het ticketingsysteem van de Leverancier voortdurend inzicht in de actuele status van het incident. Alle relevante statuswijzigingen, zoals de start van het onderzoek, escalaties, contact met derde partijen en het treffen van een oplossing, worden direct in het ticket bijgewerkt. Hierdoor kan de VRFGV op elk gewenst moment de voortgang en de genomen acties volgen.

Telefonisch contact bij elke statuswijziging is niet verplicht; het ticketingsysteem is het primaire communicatiemiddel. Alleen wanneer de situatie hierom vraagt, bijvoorbeeld bij kritieke ontwikkelingen of wanneer extra toelichting nodig is, neemt de Leverancier proactief contact op met de VRFGV. Zo blijft de communicatie efficiënt en transparant, en is de VRFGV altijd goed geïnformeerd over de afhandeling van het incident.

2.3 Inspanningsverplichting bij externe incidenten

Indien de oorzaak van een incident niet binnen de dienstverlening of invloedssfeer van de Leverancier ligt—zoals bij storingen of beperkingen bij externe leveranciers (bijvoorbeeld Microsoft of andere serviceproviders)—kan de Leverancier niet verantwoordelijk worden gehouden voor het naleven van de afgesproken oplostijden. In deze situaties blijft de Leverancier echter actief betrokken door de voortgang van het incident te bewaken en de VRFGV regelmatig te informeren over de status, de acties van de externe partij en de verwachte hersteltermijn. Zo blijft de VRFGV op de hoogte, ook wanneer de oplossing afhankelijk is van derden.

2.4 Definities per type incident en voorbeelden

Voor elk incidenttype volgt een korte toelichting, zodat helder is wat onder de verschillende categorieën wordt verstaan. Ter illustratie zijn er voorbeelden opgenomen die een beeld geven van situaties die onder een bepaald incidenttype kunnen vallen. Deze voorbeelden zijn niet uitputtend of bindend, maar dienen uitsluitend om de Leverancier inzicht te geven in de aard en impact van de verschillende incidenten

Prio 1 (P1) – Kritisch

Prio1-incidenten zijn kritieke situaties die direct de continuïteit, veiligheid of dienstverlening van de organisatie bedreigen. Bij deze incidenten is er geen werkbare alternatieve oplossing beschikbaar en is onmiddellijke actie vereist om ernstige gevolgen voor de bedrijfsvoering te voorkomen. P1-incidenten krijgen de hoogste prioriteit en vereisen directe inzet van alle betrokken partijen om zo snel mogelijk tot een oplossing te komen.

Voorbeeld 1	Een ransomware-aanval waardoor alle bedrijfsdata direct wordt versleuteld en het volledige bedrijf stilvalt.
Voorbeeld 2	Uitval van de Core Switch, waardoor het volledige netwerk platligt en geen enkele medewerker meer kan werken.
Voorbeeld 3	Uitval van de telefooncentrale of internetverbinding voor de hele organisatie. Geen enkele medewerker kan werken of communiceren, zowel intern als extern.
Voorbeeld 4	Servercrash van een bedrijf kritisch systeem.
Voorbeeld 5	Uitval van kritische cloudomgevingen (zoals Azure of Microsoft 365) waardoor alle bedrijfsapplicaties wereldwijd onbereikbaar zijn.

Prio 2 (P2) – Hoog

P2-incidenten zijn situaties waarbij een incident aanzienlijke impact heeft op een afdeling, locatie of een grote groep gebruikers. Hoewel de organisatie als geheel niet volledig tot stilstand komt, ondervinden betrokken medewerkers wel substantiële hinder in hun werkzaamheden. In veel gevallen is het mogelijk om (gedeeltelijk) door te werken, bijvoorbeeld door gebruik te maken van een tijdelijke workaround. Deze incidenten vereisen snelle opvolging en prioriteit, zodat de impact op de bedrijfsvoering zoveel mogelijk wordt beperkt.

Voorbeeld 6	Uitval van een netwerkcomponent waardoor een afdeling geen netwerktoegang heeft.
Voorbeeld 7	Segmentatieprobleem (VLAN) waardoor een afdeling geen toegang heeft tot bedrijfsnetwerken of cloudapplicaties, terwijl anderen wel kunnen werken.
Voorbeeld 8	Gedeeltelijke uitval van de internetverbinding, waardoor bijvoorbeeld alleen het gastennetwerk of een afdeling offline is, terwijl de bedrijfsvoering doorgaat.
Voorbeeld 9	Storing in authenticatie- of autorisatieketen (zoals Entra ID) waardoor een afdeling geen toegang heeft tot cloudapplicaties, terwijl anderen wel kunnen werken.
Voorbeeld 10	Problemen met Single Sign-On (SSO) waardoor een specifieke groep gebruikers niet kan inloggen op bedrijfsbrede cloudapplicaties, maar anderen wel.

Prio 3 (P3) – Midden

P3-incidenten zijn minder urgente situaties die een beperkte impact hebben op individuele gebruikers of systemen die niet essentieel zijn voor de primaire bedrijfsvoering. Het betreft bijvoorbeeld storingen of problemen waarbij het werk grotendeels kan doorgaan en er vaak een tijdelijke oplossing (workaround) beschikbaar is. Deze incidenten vragen om opvolging, maar hebben geen directe gevolgen voor de continuïteit van de organisatie.

Voorbeeld 11	Een medewerker kan niet inloggen in Teams, terwijl andere gebruikers geen problemen ervaren.
Voorbeeld 12	Een medewerker heeft geen toegang tot een gedeelde mailbox of distributielijst, maar kan wel e-mailen via het eigen account.
Voorbeeld 13	Een medewerker kan geen verbinding maken met het WiFi-netwerk op een specifieke werkplek
Voorbeeld 14	Een storing op een enkele netwerkpoort van een switch, waardoor één werkplek of apparaat geen netwerkverbinding heeft.
Voorbeeld 15	Een medewerker krijgt een certificaatfoutmelding op de laptop bij het openen van een bedrijfsapplicatie, terwijl andere gebruikers geen problemen ervaren.

Prio 4 (P4) – Laag

P4-incidenten zijn verzoeken of incidenten met een minimale impact op de organisatie, waarbij de bedrijfsvoering niet wordt verstoord. Het gaat vaak om cosmetische problemen, gebruiksvriendelijke aanpassingen of niet-essentiële wijzigingen die geen invloed hebben op de continuïteit of veiligheid van de dienstverlening. Deze meldingen kunnen zonder urgentie worden opgepakt en hebben een lagere prioriteit binnen het incidentmanagementproces.

Voorbeeld 16	Een gebruiker meldt dat een knop of tekst niet goed wordt weergegeven in een Office applicatie, maar de functionaliteit werkt verder correct.
Voorbeeld 17	Een verkeerd logo, kleur of lay-out op het Intranet of in een Dashboard zonder dat dit het gebruik belemmert.
Voorbeeld 18	Een tijdelijke uitval van een testomgeving of een niet-productie gerelateerd systeem.
Voorbeeld 19	Een niet-essentiële koppeling tussen systemen werkt tijdelijk niet, bijvoorbeeld een koppeling met een archiefmodule die niet direct nodig is voor dagelijkse processen.
Voorbeeld 20	Een rapportage in een Dashboard toont een verkeerde datum of naam, maar de cijfers en functionaliteit zijn correct.

3. Changemanagement

3.1 Changeclassificatie, doorlooptijden en goedkeuringsprocedures

Changes worden geclassificeerd op basis van impact, urgentie en complexiteit. Voor elk type change gelden specifieke doorlooptijden en procedures.

Type change	Definitie	Standaard doorlooptijd	Procedure & goedkeuring	Norm
Emergency Change	Change met hoge urgentie, noodzakelijk voor het oplossen van een crisis of P1-incident.	Direct (binnen 4 uur)	Versnelde procedure, ECAB, minimale documentatie, direct overleg.	95% per maand binnen doorlooptijd
Standard Change	Repeterende, laag-risico change met vooraf bekende uitkomst.	1-3 werkdagen	Geautomatiseerd, vooraf goedgekeurd, uitgevoerd door Servicedesk.	95% per maand binnen doorlooptijd
Minor Change	Niet-standaard change met beperkte impact, vereist risicoanalyse.	3-5 werkdagen	Autorisatie door change manager, overleg met stakeholders.	95% per maand binnen doorlooptijd
Major Change	Change met grote impact of complexiteit, mogelijk effect op continuïteit.	5-10 werkdagen	Change Advisory Board (CAB), uitgebreide impactanalyse, planning.	90% per maand binnen doorlooptijd

3.2 Statusupdates en communicatie

De VRFGV heeft via het ticketingsysteem continu inzicht in de status van alle openstaande changes. Bij het uitvoeren van een emergency change wordt de VRFGV regelmatig op de hoogte gehouden van de voortgang door middel van statusupdates, zodat eventuele ontwikkelingen direct inzichtelijk zijn. In het geval van een crisis of wanneer de voortgang afhankelijk is van derden, wordt de VRFGV proactief geïnformeerd over de voortgang, eventuele knelpunten en de verwachte opleverdatum.

3.3 Inspanningsverplichting bij externe changes

Indien de uitvoering of afronding van een change afhankelijk is van externe leveranciers of serviceproviders (zoals Microsoft of andere derde partijen), is de Leverancier niet gehouden aan de overeengekomen doorlooptijd voor deze change. In dergelijke gevallen zal de Leverancier zich inspannen om de voortgang van de change actief te bewaken, de VRFGV tijdig en proactief te informeren over de status, knelpunten en verwachte opleverdatum, en waar mogelijk de externe partij aan te sturen om het proces te versnellen.

3.4 Change Management Proces

Het change management proces bestaat uit een aantal gestructureerde stappen die zorgen voor een gecontroleerde en transparante afhandeling van wijzigingen binnen de ICT-omgeving. Elke wijziging start met een Request for Change (RFC), waarin een duidelijke beschrijving, de verwachte impact, de risico's en een rollback-plan worden opgenomen. Vervolgens beoordeelt de change manager de aanvraag en wordt het type change geclassificeerd.

Voor minor, major en emergency changes wordt een uitgebreide impact- en risicoanalyse uitgevoerd om mogelijke gevolgen in kaart te brengen. Standard changes zijn vooraf goedgekeurd, terwijl minor en major changes ter beoordeling worden voorgelegd aan de change manager of de Change Advisory Board (CAB). Emergency changes worden beoordeeld door de Emergency Change Advisory Board (ECAB).

Na goedkeuring worden de changes ingepland, worden de relevante stakeholders geïnformeerd en worden de communicatiekanalen vastgesteld. De uitvoering van de change vindt plaats volgens het goedgekeurde plan. Na de uitvoering wordt gecontroleerd of de wijziging correct is doorgevoerd door middel van testen en validatie. Alle stappen en uitkomsten worden zorgvuldig gedocumenteerd. Na major en emergency changes volgt bovendien een evaluatie om het proces en de resultaten te beoordelen en waar nodig verbeteringen door te voeren.

3.5 Best Practices en borging

Alle changes worden systematisch gepland, uitgevoerd en geëvalueerd volgens de ITIL-standaarden. In het proces wordt gewerkt met changetemplates, de inzet van de Change Advisory Board (CAB) of Emergency Change Advisory Board (ECAB), en een vooraf bepaalde rollback-procedure. Documentatie, communicatie en risicobeheersing zijn vaste onderdelen van het changeproces. Daarnaast vindt er minimaal één keer per half jaar een evaluatie van het changeproces plaats, gericht op continue verbetering.

3.6 Definities per type change en voorbeelden

Voor elk type change volgt een korte toelichting, zodat duidelijk is wat onder de verschillende categorieën wordt verstaan. Ter illustratie zijn er voorbeelden opgenomen die een beeld geven van situaties die onder een bepaald changetype kunnen vallen. Deze voorbeelden zijn niet uitputtend of bindend, maar dienen uitsluitend om de Leverancier inzicht te geven in de aard en impact van de verschillende changes.

Emergency Change

Een emergency change is een niet-planbare, direct noodzakelijke wijziging aan Microsoft 365, Azure of netwerkcomponenten, die als reactie op een incident of acute dreiging wordt doorgevoerd om de dienstverlening, bedrijfscontinuïteit of beveiliging te herstellen of te waarborgen. Deze changes zijn vaak het gevolg van onverwachte situaties, zoals ernstige storingen, beveiligingsincidenten of dreigingen die onmiddellijke actie vereisen. Omdat de impact op de organisatie groot kan zijn, wordt een emergency change met de hoogste prioriteit behandeld en zo snel mogelijk uitgevoerd, vaak buiten de reguliere changeprocedures om.

Voorbeeld 1	Direct doorvoeren van een configuratiewijziging in Azure om een kritieke kwetsbaarheid te mitigeren na ontdekking van een incident.
Voorbeeld 2	Versneld uitrollen van een beveiligingspatch in Microsoft 365 na melding van een ernstige kwetsbaarheid.
Voorbeeld 3	Onmiddellijk aanpassen van toegangsrechten in Microsoft 365 om misbruik te voorkomen na een security-incident.
Voorbeeld 4	Activeren van een alternatieve configuratie in Azure om de continuïteit van een bedrijfsproces te herstellen na een storing.
Voorbeeld 5	Snel wijzigen van VLAN-instellingen om netwerksegmenten te isoleren na een geconstateerde dreiging.

Standard Change

Een standaard change is een vooraf goedgekeurde, repeterende wijziging met een laag risico en een voorspelbaar resultaat binnen Microsoft 365, Azure of netwerkcomponenten. Deze changes maken deel uit van het reguliere beheer en worden volgens vaste, gestandaardiseerde procedures uitgevoerd. Omdat het om routinematige aanpassingen gaat waarvan de impact en uitkomst vooraf duidelijk zijn, is er geen aparte goedkeuringsronde nodig.

Voorbeeld 6	Periodieke firmware-updates van switches en access points.
Voorbeeld 7	Geautomatiseerde installatie van beveiligingspatches op werkplekken via Intune.
Voorbeeld 8	Toevoegen van een nieuwe gebruiker aan Microsoft 365 met standaard rechten.
Voorbeeld 9	Uitrollen van vooraf goedgekeurde software-updates op servers.
Voorbeeld 10	Toevoegen van een extra mailbox of distributielijst.

Minor Change

Een minor change is een niet-standaard wijziging met beperkte impact op dienstverlening of gebruikers binnen Microsoft 365, Azure of netwerkcomponenten. Deze changes vereisen een risicoanalyse en goedkeuring door de change manager, maar hebben geen grote gevolgen voor de bedrijfsvoering.

Voorbeeld 11	Configuratie van een extra printer of gedeelde map voor een team.
Voorbeeld 12	Aanpassen van gebruikersrechten voor een specifieke medewerker in Microsoft 365 en Azure.
Voorbeeld 13	Wijzigen van instellingen in een bestaande applicatie zonder grote impact.
Voorbeeld 14	Het toevoegen van een nieuwe distributielijst of het aanpassen van de leden van een bestaande lijst.
Voorbeeld 15	Toevoegen of aanpassen van een e-mailhandtekening voor een groep gebruikers.

Major Change

Een major change is een wijziging met grote impact of complexiteit binnen Microsoft 365, Azure of netwerkcomponenten, die gevolgen kan hebben voor continuïteit, beveiliging of werking van de ICT-omgeving. Major changes vereisen uitgebreide impact- en risicoanalyse, goedkeuring door de Change Advisory Board (CAB) en een gedetailleerde planning.

Voorbeeld 16	Migratie van een volledige afdeling naar een nieuwe Microsoft 365 tenant.
Voorbeeld 17	Implementatie van een nieuw netwerksegment of grote wijziging in VLAN-structuur.
Voorbeeld 18	Uitrollen van een nieuwe security-oplossing (bijvoorbeeld MFA voor alle gebruikers in Microsoft 365).
Voorbeeld 19	Integratie van een nieuwe applicatie met Single Sign-On (SSO) voor alle medewerkers.
Voorbeeld 20	Grote upgrade van de Azure-omgeving, inclusief herinrichting van resourcegroepen en subscriptions.

4. Escalatiematrix en 24x7 Bereikbaarheid P1

De escalatiematrix definieert de gestandaardiseerde route voor het opschalen van incidenten. Het proces is 24/7 beschikbaar voor kritieke (Prio 1) incidenten. Het primaire doel is het bieden van helderheid over de juiste contactpersoon, het communicatiemiddel en de maximale termijnen waarbinnen de escalatie naar een hoger besluitvormingsniveau moet plaatsvinden.

Niveau	Rol/ Functie	Bereikbaarheid	Escalatie na
1	Servicedesk Opdrachtgever	24 x 7 (telefoon)	Onmiddellijk na de registratie van de melding.
2	Incident Manager Opdrachtnemer	24 x 7 (telefoon)	Nadat 1 uur is verstreken zonder actieve opvolging van het incident.
3	Senior Systeembeheerder VRFGV	24 x 7 (telefoon)	Nadat 2 uur is verstreken zonder substantiële voortgang.
4	Teamleider ICT-afdeling VRFGV	24 x 7 (telefoon)	Binnen 1 uur na de escalatie door Niveau 3.
5	Operations Manager Opdrachtnemer	24 x 7 (telefoon)	Binnen 30 minuten nadat de escalatie is geïnitieerd door Niveau 3 én/of Niveau 4
6	CIO VRFGV / CIO Opdrachtnemer	24 x 7 (telefoon)	Bij de constatering dat een oplossing niet haalbaar is binnen een redelijke termijn OF wanneer de totale doorlooptijd 6 uur overschrijdt.