SERVICE LEVEL AGREEMENT (SLA) OG SIKKERHED

FOR

AUTO IT'S SOFTWARE AS A SERVICE LØSNINGER

[dag]. [måned] [år]

1. Indledning

1.1 Denne Service Level Agreement ("**SLA**") er en del af Aftalen mellem Kunden og Auto IT.

1.2 Formålet med SLA'en er at definere de servicemål (Service Level Targets ("**SLT**")), herunder oppetider, Support og vedligeholdelse af Tjenesterne, som leveres af Auto IT, som defineret i Aftalen. Herudover angives det aftalte niveau af sikkerhed, som Auto IT har implementeret, og som gælder for Tjenesterne.

2. Definitioner

2.1 Definitionerne og fortolkningsreglerne i dette pkt. 2 gælder i denne SLA.

Aftalen: den aftalte og underskrevne Hovedaftale sammen med disse vilkår og betingelser for Auto IT's Software as a Service løsninger, og eventuelle andre kontraktlige dokumenter, der er aftalt skriftligt mellem parterne for at være en del af Aftalen.

Prioriteringsniveau: klassificeringen af en Supportanmodning fastlagt af Auto IT, som defineret i pkt. 4.2.

Dokumentation: det dokument, som Auto IT stiller til rådighed for Kunden, som Auto IT fra tid til anden meddeler Kunden, og som indeholder en beskrivelse af Tjenesterne og brugervejledningen til Tjenesterne.

Hovedaftale: det dokument, der beskriver de overordnede vilkår mellem parterne, herunder Kundens valg af løsninger og tjenester og relaterede vilkår, som en del af Aftalen.

Kunden: den fysiske eller juridiske person eller gruppe af personer, som beskrevet i Hovedaftalen, der køber Tjenesterne fra Auto IT.

Normale Åbningstider: som defineret i Vilkår og Betingelser for Auto IT's Software as a Service Løsninger.

Auto IT: den juridiske person, som beskrevet i Hovedaftalen, der leverer Tjenesterne, som beskrevet i Hovedaftalen.

Support: den assistance, som Auto IT yder til Kunden for at løse problemer, besvare spørgsmål og give vejledning i forbindelse med brugen af Tjenesterne. Dette omfatter helpdesk, fejlfinding og kundeservice, men ikke uddannelse af Kundens personale i brugen af Tjenesterne.

Supportanmodning: den anmodning om Support via helpdesk, som Kunden har anmodet i forbindelse med problemer med eller spørgsmål til Tjenesterne.

Responstid: den tid inden for Normale Åbningstider fra modtagelse af en Supportanmodning fra Kunden, indtil Auto IT påbegynder håndtering af Supportanmodningen med en personlig (ikke-automatisk) besked.

Tjenester: de tjenester, som Auto IT leverer til Kunden i henhold til Aftalen og vilkårene, som nærmere beskrevet i Hovedaftalen og Dokumentationen.

3. Service Level Targets (SLT'er)

3.1 Auto IT skal så vidt muligt bestræbe sig på at levere følgende SLT'er:

3.2 Tilgængelighed

- Tjenesterne skal være tilgængelig 24 / 7 / 365, med undtagelse af planlagt vedligeholdelse
- Planlagt vedligeholdelse kan udføres alle dage mellem kl. 20.00 – 06.00. Yderligere vedligeholdelsesperioder kan varsles med minimum ti (10) dages varsel.
- Nødvedligeholdelse, f.eks. i forbindelse med opdagelse af kritiske og akutte sårbarheder, kan gennemføres når som helst og uden varsel.

3.3 Oppetid

- Tjenesterne har en tilstræbt oppetid på 99,8 %, med undtagelse af planlagt vedligeholdelse og forhold uden for Auto IT's direkte kontrol, herunder force majeure hændelser.

3.4 Åbningstider

- Kunden skal kunne modtage Support inden for Normale Åbningstider.

4. Responstid for Support

4.1 Følgende Responstider for Support er gældende i denne SLA:

Prioritetsniveau	Responstid
Høj prioritet	2 timer
Mellem prioritet	8 timer
Lav prioritet	16 timer

4.2 Prioriteringsniveauerne for Responstid er defineret nedenfor:

- **Høj prioritet**: Tildeles en sag i de tilfælde, hvor Kunden ikke kan benytte Tjenesterne til normal afvikling af driften. Dette kan f.eks. være tilfælde, hvor en for løsningen vital server ikke fungerer, eller såfremt sagen omhandler kritiske, kundevendte funktioner, hvorved forstås de processer, hvor brugerne i den direkte dialog med Kunden er ude af stand til at komme videre i kundebetjeningen, og hvor der ikke kan anvises en hensigtsmæssig work-around løsning. Auto IT vil arbejde kontinuerligt på løsning af sagen, indtil Tjenesterne er genoprettet, eller der er anvist en hensigtsmæssig work-around.

- **Mellem prioritet**: Tildeles en sag i de tilfælde der medfører at andre forretningsmæssige væsentlige dele af systemet er ude af drift, og hændelsen har betydelige negative driftsmæssige konsekvenser for Kunden, og hvor der ikke kan henvises til en hensigtsmæssig work-around.
- **Lav prioritet**: Tildeles en sag, som er almindelige spørgsmål om funktionalitet. Det vil være sager, som ikke forhindrer brugerne i at foretage sit daglige arbejde, altså også sager hvor der tilbydes en hensigtsmæssig work-around, samt hvor brugeren er kommet videre i den konkrete sag.

5. Sikkerhedsforanstaltninger

5.1 Auto IT har implementeret følgende sikkerhedsforanstaltninger i Tjenesterne for at sikre et passende niveau af sikkerhed. Auto IT kan fastsætte yderligere sikkerhedsforanstaltninger eller foretage ændringer til de implementerede sikkerhedsforanstaltninger, såfremt der fortsat opretholdes et passende niveau af sikkerhed.

5.2 Organisatoriske sikkerhedsforanstaltninger

- Alle medarbejdere har en almindelig brugerprofil. Kun relevante medarbejdere har en administrationsprofil.
- Medarbejdere må ikke dele personlige profiler og adgangskoder med andre.
- Adgange er tildelt efter et nødvendighedsprincip.
- Tildeling af adgang revideres mindst én (1) gang hvert halve (½) år.
- Medarbejdere oplæres i anti-malware.
- Medarbejdere oplæres i opdateringer til operativsystemer.
- Medarbejdere oplæres i opdateringer til anvendt software.
- Medarbejdere oplæres i at kende og imødegå IT-trusler.
- Kontorfaciliteterne har aflåste adgangsveje.
- Kontorfaciliteterne har alarm aktiveret, når der ikke er medarbejdere til stede.
- Kontorfaciliteterne har videoovervågning ved hovedindgangen.
- Adgang til kontorfaciliteterne er givet personligt for relevante personer ved brug af personlige adgangskort og koder.
- Alle medarbejdere har underskrevet en tavshedserklæring.
- Der er en beredskabsplan for genoprettelse af driften i tilfælde af en hændelse.
- Sikkerhedsniveauet bliver vurderet mindst én (1) gang årligt.
- Sikkerhedsorganisationen koordinerer sikkerhedsarbejdet og -opgaverne mindst én (1) gang pr. kvartal.
- Informationer om sikkerhed fra brancheorganisationer, rådgivere og lignende indhentes løbende.

- I udviklingsprocessen benyttes opgaveskabeloner, der indeholder ikke-funktionelle krav, herunder sikkerhed, logning og adgangsstyring.

5.3 Tekniske sikkerhedsforanstaltninger

- Adgangsstyring og styring af brugerprofiler skal ske gennem et fælles, almen anerkendt, system for administration af brugerprofiler.
- Almindelige brugerprofiler benytter flerfaktorgodkendelse.
- Adgangskoder er underlagt kompleksitetskrav.
- Alle brugerprofiler skifter adgangskoden jævnligt og mindst hver tredje (3.) måned.
- Adgang til netværk kan kun ske med for profiler i systemet for administration af brugerprofiler, med undtagelse af netværkssegmenterne til besøgende og mobile enheder/IoT.
- Adgang til udstillede services fra internettet sker gennem firewall.
- Firewall er så restriktivt konfigureret, som muligt.
- Adgang til interne miljøer og systemer for medarbejdere sker via adgang på kontoret eller via firewall, samt VPN med flerfaktorgodkendelse.
- Administrationsprofiler kan ikke logge på via VPN.
- Adgange til produktionsservere og produktionsdata sker med administrationsprofiler, som ikke er den almindelige brugerprofil.
- Transmission af data på internettet er krypteret efter en almen anerkendt standard.
- Domain Name System Security (DNSSEC) anvendes.
- Domain-based Message Authentication, Reporting & Conformance (DMARC) anvendes.
- Wi-Fi anvender WPA2.
- Security Information & Event Management (SIEM) system anvendes på både firewall, e-mails, arbejdsstationer og servere.
- Hosting sker i et alment anerkendt hostingcenter.
- Hosting må ikke finde sted i Auto IT's kontorfaciliteter.
- Produktionsservere kan være underlagt dobbelt-hosting.
- På servere og arbejdsstationer er der aktivt, opdateret og almen anerkendt anti-malware installeret.
- Operativsystemer opdateres mindst én (1) gang månedligt.
- Applikationer opdateres mindst én (1) gang månedligt.
- Indhold på harddiske er krypteret.
- Indhold på eksterne medier er krypteret.

- På servere tages der fuld sikkerhedskopi af filer dagligt. Sikkerhedskopier er tilgængelige i mindst tredive (30) dage.