



CitizenOne - Service Level Agreement (SLA)

Version: 1.0
Gældende fra: 2026
Leverandør: CitizenOne A/S
System: CitizenOne

KOMMERCIELT FORTROLIGT

Denne SLA udgør en integreret del af aftalen mellem CitizenOne A/S (herefter "Leverandøren") og Kunden.

1. Formål

Denne Service Level Agreement beskriver de service- og driftsniveauer, som CitizenOne A/S leverer i forbindelse med drift af CitizenOne-platformen.

Formålet er at sikre:

- høj tilgængelighed
- stabil drift
- sikker håndtering af data
- klare support- og incident-procedurer

CitizenOne anvendes i social- og sundhedssektoren, og systemet er derfor designet med høje krav til driftssikkerhed, databeskyttelse og compliance.

2. Systemets tilgængelighed

CitizenOne tilstræber en månedlig opetid på minimum 99,5 %, eksklusivt planlagt vedligehold, force majeure, tredjepartsfejl og forhold uden for Leverandørens kontrol.

Opetid beregnes ekskl. planlagt vedligehold.

Planlagt vedligehold:

- varsles minimum 48 timer før
- udføres typisk uden for normal arbejdstid

3. Support

Mandag - torsdag: 09:00 - 16:00 via chat og mail

Fredag: 09:00 - 15:00 via chat og mail

Mandag - torsdag: 10:00 - 14:00 via telefon (minimum Pro abn.)

Fredag: 10:00 - 14:00 via telefon (minimum Pro abn.)



Prioritering af support:

Prioritet	Beskrivelse	Reaktionstid
Kritisk	Kritisk fejl der forhindrer brug af systemet for størstedelen af brugerne	Fejlretning påbegyndes senest 2 timer efter modtagelse
Høj	Alvorlig fejl der påvirker væsentlige funktioner eller mange brugere	Fejlretning påbegyndes senest 4 timer efter modtagelse
Normal	Mærkbar fejl der påvirker en mindre gruppe brugere	Fejlretning påbegyndes senest 8 timer efter modtagelse

3.1 Generel support

Kunden har som en del af sin aftale adgang til grundlæggende support vedrørende Leverandørens software. Dette inkluderer:

- Fejlregistrering og kategorisering
- Vurdering af problemets omfang og indsamling af relevante oplysninger
- Grundlæggende fejlsøgning og genstart af services
- Konsulentbistand kan være fakturerbar i henhold til gældende prisliste



3.2 Fejlkategorier og reaktionstider

Reaktionstid angiver tidspunktet hvor fejlfhjælpning påbegyndes, ikke hvornår problemet nødvendigvis er løst.

Fejl klassificeres i fem kategorier:

Kategori	Beskrivelse	Reaktionstid
C1	Kritisk fejl der forhindrer brug af systemet for størstedelen af brugerne	Fejlretning påbegyndes senest 2 timer efter modtagelse
C2	Alvorlig fejl der påvirker væsentlige funktioner eller mange brugere	Fejlretning påbegyndes senest 4 timer efter modtagelse
C3	Mærkbare fejl der påvirker en mindre gruppe brugere	Fejlretning påbegyndes senest 8 timer efter modtagelse
C4	Mindre fejl der påvirker enkeltfunktioner	Fejlretning påbegyndes senest 2 arbejdsdage efter modtagelse
C5	Mindre fejl uden væsentlig forretningseffekt	Fejl håndteres i kommende opdateringer

3.3 Teknisk support

Ved behov for kodeændringer eller avanceret fejlretning påbegyndes arbejdet som følger:

Kategori	Beskrivelse	Reaktionstid
P1	Kritisk fejl uden workaround	Udbedres straks
P2	Kritisk fejl med midlertidig workaround	Udbedres i næste rettelsesrelease
P3	Ikke-kritisk fejl	Planlægges i kommende opdateringer

4. Incident Management

CitizenOne har en dokumenteret proces for håndtering af sikkerheds- og driftsincidenter.



Ved kritiske hændelser:

- Kunden informeres hurtigst muligt og som udgangspunkt inden for 1 time ved kritiske sikkerhedshændelser
- Statusopdateringer gives løbende
- Root cause analyse gennemføres efterfølgende

Ved sikkerhedsbrud håndteres rapportering i henhold til:

- GDPR
- NIS2 hvor relevant
- gældende lovgivning

5. Drift og overvågning

CitizenOne overvåger platformen løbende.

Overvågning inkluderer:

- systemtilgængelighed
- serverressourcer
- databaseperformance
- sikkerhedshændelser

Drift overvåges 24/7 via automatiske monitoreringssystemer.

6. Backup og gendannelse

CitizenOne anvender en backupstrategi baseret på 3-2-1 princippet.

Dette indebærer:

- flere backupkopier
- geografisk adskilte lagringssteder
- krypterede backups
- RTO (Recovery Time Objective): op til 24 timer
- RPO (Recovery Point Objective): op til 24 timer

Backup foretages:

- dagligt
- med løbende restore-tests

7. Databeskyttelse

CitizenOne håndterer data i overensstemmelse med:

- GDPR
- databehandleraftale
- europæisk datalovgivning

Sikkerhedstiltag inkluderer:

- kryptering af data i transit
- kryptering af data i hvile



- rollebaseret adgangsstyring
- logning af systemadgange

Data hostes som udgangspunkt inden for EU.

8. Adgangsstyring

CitizenOne anvender følgende principper:

- unikke brugeridentiteter
- rollebaseret adgang
- least privilege-princip
- mulighed for multifaktorautentificering

Adgange gennemgås løbende.

9. Logning og audit

Systemet logger relevante hændelser for at sikre sporbarhed.

Dette omfatter blandt andet:

- loginforsøg
- brugerrettighedsændringer
- systemændringer
- API-integrationer
- sikkerhedshændelser

Logdata opbevares i henhold til gældende sikkerhedspraksis.

10. Infrastruktur og sikkerhed

CitizenOne anvender moderne sikkerhedsforanstaltninger, herunder:

- firewalls
- intrusion detection
- antivirus / EDR
- sårbarhedsscanning

Kritiske sikkerhedsopdateringer installeres løbende.

11. Systemudvikling

CitizenOne udvikles efter principper for Secure Software Development Lifecycle (Secure SDLC).

Dette inkluderer:

- adskillelse mellem udvikling, test og produktion
- versionsstyring
- change management
- release-logning



12. Underleverandører

CitizenOne anvender udvalgte underleverandører til hosting og drift.

Disse leverandører er underlagt:

- databehandlaftaler
- sikkerhedskrav
- løbende vurdering

13. Business Continuity

CitizenOne har etableret procedurer for:

- disaster recovery
- business continuity
- gendannelse af systemer ved nedbrud

Dette sikrer hurtig genetablering af platformen ved kritiske hændelser.

14. Revision og compliance

CitizenOne arbejder løbende med:

- sikkerhedsrevision
- compliance
- forbedring af sikkerhedsprocesser

Efter aftale kan kunder få adgang til relevant dokumentation.

15. Ophør af aftale

Ved ophør af aftalen:

- kundedata returneres efter aftale
- eller slettes sikkert
- alle systemadgange lukkes

Dokumentation for sletning kan leveres.

16. Ansvarsbegrænsning

CitizenOne tilstræber høj stabilitet og sikkerhed, men kan ikke garantere uafbrudt drift i alle situationer.

Eventuelle erstatningsforhold reguleres i kundens hovedaftale. Leverandøren kan ikke holdes ansvarlig for indirekte tab, driftstab, tabt fortjeneste eller følgeskader.