Workplace Safety

Standard tjenestenivåavtale (SLA) – Workplace Safety

Innhold

1. Formål og omfang

1.1 Formål

Denne Service Level Agreement (SLA) regulerer Netpower Business Solutions AS' leveranse av Workplace Safety som tjeneste. Avtalen skal sikre høy kvalitet, stabil drift, effektiv support, robust informasjonssikkerhet og forutsigbarhet for kunden. SLA'en tydeliggjør både Netpowers forpliktelser og kundens ansvar, og er en del av vårt ISO 27001-sertifiserte styringssystem for informasjonssikkerhet (ISMS).

1.2 Omfang

Avtalen dekker:

- Drift av applikasjonen i Netpowers datasentre, inkludert overvåking og vedlikehold av infrastruktur.
- Vedlikehold, forvaltning og videreutvikling av selve applikasjonen, herunder kildekode, programrettelser, sikkerhetspatching, oppdateringer og tilgjengeliggjøring av nye versjoner.
- Brukerstøtte, feilsøking og feilretting i henhold til definerte kritikalitetsnivåer.
- Oppetidsgaranti og kompensasjonsordninger.
- Prosess for håndtering av supportsaker fra registrering til lukking.
- Opsjon for utvidet vakttelefon med døgnkontinuerlig beredskap.
- Spesifikke bestemmelser for skreddersydd funksjonalitet og drift på kundens infrastruktur.
- Spesifikke bestemmelser for sikkerhetsdatablader (SDS) og kjemikaliedata.
- Spesifikke bestemmelser for eksponeringsregisteret.

2. Definisjoner

- **Oppetid:** Tid tjenesten er tilgjengelig fra Netpowers ytterste nettknutepunkt til applikasjonsserver. Planlagt vedlikehold og unntak etter punkt 9 omfattes ikke.
- **Responstid:** Tiden fra sak registreres i Zendesk til feilsøking er påbegynt. SLA garanterer oppstart av feilsøk, ikke løsningstid.
- **Kritikalitetsnivåer:** P1 (kritisk), P2 (høy), P3 (medium), P4 (lav), jf. punkt 6.
- **ISMS:** Netpowers styringssystem for informasjonssikkerhet, sertifisert etter ISO 27001.
- **Skreddersydd funksjonalitet:** Funksjoner eller visninger utviklet særskilt for en kunde, og som ikke inngår i standardversjonen.
- **Kundedriftet infrastruktur:** Tilfeller der applikasjonen driftes på kundens eget miljø eller datasenter i stedet for Netpowers datasentre.

3. Driftsmiljø og sikkerhet

Netpower leverer drift fra egne datasentre i Sandnes, med høy grad av fysisk og logisk sikring.

3.1 Fysisk og logisk sikkerhet

- Adgangskontroll (personlig kort og kode), vekterpatruljering, video- og bevegelsesovervåkning.
- Redundant strømtilførsel (UPS og dieselgenerator med autostart).
- Redundant kjøling og kontinuerlig klimakontroll.
- Brann- og fuktighetsdetektorer samt Inergen brannslukningsanlegg.

3.2 Infrastruktur og redundans

- Mulighet for High Availability (HA) med lastbalansering og failover-konfigurasjon.
- Redundant nettverk med minst to uavhengige linjer mot internett.
- Infrastruktur designet for høy tilgjengelighet og rask gjenoppretting ved feil.

3.3 Serverdrift og patching

- Alle servere driftes med etablerte rutiner for operativsystem- og sikkerhetspatching.
- Kritiske oppdateringer og zero-day sårbarheter håndteres med forsert patching utenom ordinært servicevindu dersom risiko tilsier det.
- IDS/IPS-regler, antivirus og antimalware oppdateres løpende.
- Brannmurer konfigureres etter prinsippet om «least privilege» og oppdateres kontinuerlig med nye signaturer.

3.4 Overvåking og hendelseshåndtering

- Servere, nettverk og tjenester overvåkes kontinuerlig med automatiske alarmer for nedetid, ytelse og sikkerhetshendelser.
- Hendelser håndteres etter etablerte prosedyrer i Netpowers ISMS, inkludert logging, analyse og eskalering ved behov.
- Kritiske hendelser varsles umiddelbart og behandles i henhold til SLA.

Alle disse tiltakene inngår i Netpowers ISO 27001-sertifiserte ISMS. Driftsmiljø og sikkerhetsrutiner revideres årlig og oppdateres fortløpende for å møte nye trusler, sårbarheter og regulatoriske krav.

4. Supportmodell, åpningstider og kanaler

4.1 Supportnivåer

- **1.linje servicedesk:** Mottak av henvendelser, triagering, brukerstøtte og enklere feilretting.
- **2.linje:** Applikasjonsspesialister og systemteknikere med kompetanse på driftsmiljø og applikasjon.
- **3.linje:** Utviklere og arkitekter med inngående kompetanse på applikasjonsarkitektur og kode.

I tillegg til den ordinære supportmodellen tilbys kundene et omfattende selvhjelpsapparat:

- **Hjelpesider** tilgjengelig via kundeportal.workplacesafety.no, med oppdatert dokumentasjon og brukerveiledninger.

- **Opplæringsvideoer** tilgjengelig via hjelpesidene og ofte integrert direkte i kundens egen applikasjon.
- **Kontekstuell hjelp i applikasjonen:** Applikasjonen har innebygde tooltips og hjelpeikoner (!) i visningssettene

Under implementering og prosjektfase har kunden direkte tilgang til prosjektteamet, inkludert konsulenter og utviklere, og skal i denne perioden ikke benytte servicedesken for prosjektrelaterte spørsmål.

4.2 Åpningstider og kanaler

Servicedesk er bemannet hverdager 08:00–16:00. Supportsenteret nås i denne periode på telefon 51 95 80 00, på e-post: support@workplacesafety.no eller support@netpower.no og via vårt online supportsystem enten ved at en oppretter sak eller via live chat.

- Primær kanal er Zendesk (online supportsystem).
- E-post og telefon kan benyttes, men linnkommende eller utgående henvendelser logges alltid i Zendesk.
- Ved stor pågang rutes telefonkø til ekstra personell for å redusere ventetid.

5. Prosess for supportsaker

Alle supportsaker behandles etter en etablert prosess i Netpowers servicedesk. Prosessen sikrer at saker vurderes, prioriteres og følges opp på en forutsigbar måte, og at kunden alltid holdes orientert.

1. Kunde registrerer sak i Zendesk (primær kanal). Alternativt via e-post eller telefon, logges alltid i Zendesk.
2. Ticket-ID opprettes og kunden mottar automatisk kvittering med tid og referanse.
3. Alle saker overvåkes fortløpende av servicedesk-personell gjennom hele dagen. Kritikalitet (P1–P4) vurderes umiddelbart når saken er registrert.
4. Feilsøking påbegynnes av 1. linje. Dersom feilen ikke kan løses der, eskaleres saken til 2. eller 3. linje med utført arbeid dokumentert.
5. **P1-saker** eskaleres umiddelbart og gis høyeste prioritet. Netpower setter inn de best egnede ressursene med en gang, herunder produktansvarlige (product owners) og systemarkitekter, slik at den samlede kompetansen mobiliseres raskt. Andre oppgaver settes til side til saken er under kontroll.
6. Kommunikasjon: All kommunikasjon om en supportsak skjer i Netpowers supportsystem (Zendesk). Dette sikrer full oversikt, historikk og sporbarhet for både kunden og Netpower. Ved P1-saker kan telefon benyttes i tillegg for rask avklaring, men alle oppdateringer og beslutninger loggføres alltid i Zendesk.
7. For større kunder kan Netpower fasilitere at kundens systemansvarlige har tilgang til å se og følge alle saker registrert fra organisasjonen. Dette gir oversikt over status og utvikling, og bidrar til at eventuelle kostnader aldri kommer som en overraskelse.
8. Når saken er løst, bekreftes lukking med kunden. Dokumentasjon og beskrivelse av løsning leveres dersom dette er påkrevd eller ønsket.
9. Sikkerhetsrelaterte P1-hendelser behandles også som informasjonssikkerhetshendelser i tråd med ISMS-prosedyre for hendelseshåndtering, inkludert varsling, rotårsaksanalyse og korrigerende tiltak.

6. Kritikalitet og responstid (oppstart feilsøk)

Responstid er tiden fra saken er registrert i Zendesk til feilsøking er påbegynt. SLA garanterer oppstart av feilsøking, ikke løsningstid.

Kritikalitet	Ordinær SLA (08–16)	Utvidet SLA (opsjon med vakttelefon)	Beskrivelse og typiske tilfeller
P1 Kritisk	1 time	30 min (24/7)	Total nedetid eller utilgjengelighet av applikasjonen. Ingen brukere kan logge inn eller gjennomføre kritiske prosesser. Kritiske sikkerhetshendelser som truer konfidensialitet, integritet eller tilgjengelighet av data. Eksempel: Hele systemet nede, database utilgjengelig, alvorlig databrudd.
P2 Høy	2 timer	1 time (24/7)	Vesentlig funksjonalitet ute av drift for mange brukere, men ikke total nedetid. Midlertidige løsninger finnes, men påvirker forretningskritiske prosesser. Eksempel: Oppretting av ny lokasjon fungerer ikke, store ytelsesproblemer som hindrer arbeid, integrasjon mot kritisk tredjepart feiler.
P3 Medium	4 timer	4 timer (08–22, inkl. helg)	Funksjonalitet er redusert eller påvirker enkelte brukere, men kjerneprosesser fungerer fortsatt. Ikke forretningskritisk. Eksempel: Feil i rapportfunksjon, begrensede ytelsesproblemer, feil i enkeltmoduler som har workaround.
P4 Lav	1 dag	N/A	Kosmetiske feil, brukerspørsmål, mindre feil eller forbedringsønsker som ikke påvirker driften. Eksempel: Feil i skjermtekst, oppsett av ny bruker, ønsket justering av konfigurasjon.

Feil relatert til brukersynkronisering og tilgangsstyring

Workplace Safety kan integreres med kundens identitetsmiljø (f.eks. Azure AD eller andre AD-løsninger) ved bruk av standarder som SCIM. I slike tilfeller kan tilgangsproblemer skyldes forhold utenfor selve applikasjonen, eksempelvis endringer i kundens identitetsregister, synkroniseringsrutiner eller konfigurasjon.

- Feil som kan henføres til kundens identitetsmiljø regnes ikke som applikasjonsfeil i denne SLA.
- Responstid og kritikalitet for slike saker vurderes i dialog mellom Netpower og kunden, og klassifiseres i henhold til faktisk årsak og konsekvens.
- Netpower bistår med feilsøking og veiledning for å avdekke årsak, men det operative ansvaret for drift og konfigurasjon av identitetsmiljøet ligger hos kunden.

7. Oppetidsgaranti

Netpower garanterer **99,8 % oppetid** pr. kalendermåned.

Oppetid måles fra Netpowers ytterste nettknutepunkt til applikasjonsserver. Planlagt vedlikehold og

unntak etter punkt 9 omfattes ikke.
Oppetidsmåling og avviksrapportering inngår i ISMS og kan gjøres tilgjengelig for revisjon.

8. Servicevindu

Primært onsdag 23:59–05:59. Det er ikke automatikk i nedetid i dette intervallet; Netpower tilrettelegger for minst mulig påvirkning.

9. Unntak fra oppetidsmåling

Følgende regnes ikke som brudd på oppetidsgaranti:

- Nedetid forårsaket av kunden selv eller feil i kundens utstyr.
- Nedetid på kundens forespørsel.
- Force majeure / naturkatastrofer.
- Omstarter, sikkerhetsoppdateringer og vedlikehold.

10. Kompensasjon ved SLA-brudd

Netpower er forpliktet til å levere tjenestene i tråd med denne SLA, og vi tar ansvar dersom leveransen ikke holder de definerte målene. For å gi kunden forutsigbarhet og trygghet er det etablert følgende kompensasjonsordning:

- Dersom **oppetidsgarantien på 99,8 %** ikke oppnås i en kalendermåned, eller
- Dersom **mindre enn 90 % av saker** i måneden håndteres innenfor de avtalte responstidene,

… vil kunden motta en automatisk kompensasjon i form av kreditering på månedlig vederlag.

Kompensasjonsnivå:

- 5 % reduksjon i månedsvederlaget per brudd.
- Samlet kompensasjon per måned er begrenset til 15 % av månedlig vederlag.

Prinsipper:

- Kompensasjonen er ment å reflektere redusert tjenestekvalitet og gi kunden økonomisk balanse ved avvik.
- Kreditering skjer på påfølgende faktura, tydelig spesifisert som egen linje.
- Kompensasjonen er standardisert og automatisk, slik at kunden slipper å fremme særskilt krav.
- Denne ordningen er en minimumssikring for kunden, og kommer i tillegg til de rettigheter kunden har etter hovedavtalen.

11. Backup og disaster recovery

- Netpower tar daglig backup av produksjonsdata. Standard hosting inkluderer 7 dagers oppbevaring før overskriving. Kunden kan bestille utvidet lagring på inntil 21 dager mot tillegg.
- Gjenopprettingstester gjennomføres periodisk og iht. etablerte rutiner i vårt ISO 27001-sertifiserte ISMS. Resultater dokumenteres og vurderes som en del av årlig revisjon.
- Disaster recovery-planer er etablert, dokumentert og inngår i ISMS. Planene revideres årlig, og testing gjennomføres i samsvar med risikovurdering og kundebehov.

12. Endringshåndtering og nye versjoner

- Endringsbehov registreres og estimeres fortløpende i dialog med kunden.
- Nye versjoner og oppdateringer gjøres tilgjengelig for alle lisenskunder.
- Oppgraderinger gjennomføres normalt i avtalt servicevindu og med hensyn til å bevare kundetilpasninger.
- Kunden kan velge å bli værende på eksisterende versjon i en begrenset periode, men Netpower forbeholder seg retten til å pålegge oppgradering når dette er nødvendig av hensyn til sikkerhet, stabilitet, vedlikeholdbarhet eller regulatoriske krav.
- Kritiske sikkerhetsoppdateringer og feilrettinger distribueres alltid, og kan installeres utenom servicevindu ved behov.
- Versjoner som er eldre enn en definert livssyklus (typisk 6 måneder) vil ikke lenger være støttet, og kunden plikter å oppgradere til en nyere versjon. Netpower informerer alltid i god tid om livssyklus og støtteperioder.

- Netpower sikrer at kundetilpasninger ivaretas i oppgraderingsløp, og bistår kunden med nødvendige avklaringer i forkant.
- Ved avdekking av kritiske sårbarheter eller sikkerhetsforbedringer forbeholder Netpower seg retten til å oppgradere eller patche applikasjonen utenom servicevindu. Dette gjøres for å ivareta informasjonssikkerheten og redusere risiko for driftsavbrudd eller datatap. Kunden informeres så raskt som mulig før, under og etter en slik oppgradering.

13. Skreddersydd funksjonalitet

For enkelte kunder leveres Workplace Safety med skreddersydd funksjonalitet eller tilrettelagte visninger som er utviklet særskilt for kundens behov. Slike leveranser gir stor fleksibilitet, men innebærer også særskilte forhold:

- **Feilsøking og feilretting:** Skreddersydde løsninger kan kreve lengre tid til analyse og retting enn standardfunksjonalitet, da det kan være nødvendig å involvere utviklere som kjenner den konkrete tilpasningen.

- **Oppgraderinger:** Risikoen for at skreddersydd funksjonalitet påvirkes ved oppgraderinger er høyere enn for standardversjon. Netpower vil gjøre sitt beste for å ivareta tilpasningene,

men kan ikke garantere full kompatibilitet ved alle nye versjoner. Eventuelle nødvendige justeringer avtales med kunden.

- **Responstid:** Registrerte saker på skreddersydd funksjonalitet håndteres i henhold til SLA'ens responstider, men løsningstid kan variere mer enn for standardfunksjonalitet. Kunden holdes alltid orientert om fremdrift og forventet tid til løsning.
- **Vedlikehold:** Netpower anbefaler at skreddersydde løsninger gjennomgås regelmessig sammen med kunden for å sikre kompatibilitet med ny funksjonalitet og sikkerhetsoppdateringer.

Skreddersøm gir kundene utvidet verdi, men kan medføre at support, oppgraderinger og feilretting krever mer tid og koordinering enn for standardløsningen.

14. Sikkerhet, risikovurderinger og revisjoner

- Netpower er ISO 27001-sertifisert og har etablert et ISMS.
- Årlige risikovurderinger gjennomføres av applikasjonen og driftsmiljø.
- Applikasjonen risikovurderes ved hver hovedrelease.
- Det gjennomføres årlig penetrasjonstesting av Workplace Safety.
- Kunder kan på forespørsel motta kopi av penetrasjonstester og risikovurderingsrapporter.
- Eksterne sikkerhetsrevisjoner utføres regelmessig.
- Netpower bistår kunder ved penetrasjons- og sårbarhetstester og revisjoner.

15. Sikkerhetsdatablader og kjemikaliedata

Workplace Safety inneholder database for sikkerhetsdatablader (SDS) og kjemikaliedata. Netpower tilrettelegger en sikker infrastruktur for lagring og tilgjengeliggjøring, men kunden er ansvarlig for innholdet.

Kunden skal:

- Sørge for at opplastede SDS er gyldige, oppdaterte og korrekte.
- Påse at kjemikaliedata som registreres er i samsvar med gjeldende lovverk.
- Sikre at ansatte får nødvendig opplæring i å bruke og tolke SDS.

Netpower er ikke ansvarlig for innholdet i SDS eller kjemikaliedata som lagres i systemet, men leverer en sikker og stabil plattform for håndtering av informasjonen.

16. Eksponeringsregister

Workplace Safety kan inkludere et eksponeringsregister der kunden registrerer ansatte som har vært utsatt for kjemikalier eller hendelser. Registeret kan inneholde sensitive personopplysninger, inkludert fødselsnummer og helserelatert informasjon.

- Kunden er behandlingsansvarlig for opplysninger i eksponeringsregisteret og plikter å bruke funksjonaliteten i tråd med GDPR, arbeidsmiljøregelverket og annen gjeldende lovgivning.
- Netpower er databehandler og forplikter seg til å drifte, beskytte og lagre dataene i tråd med ISO 27001 og inngått databehandleravtale.
- Kunden har ansvar for at kun nødvendige og korrekte data registreres, og at tilgang begrenses til autorisert personell.
- Netpower stiller til rådighet tekniske mekanismer som tilgangsstyring, logging og kryptering, men er ikke ansvarlig for kvaliteten i innholdet som registreres.

17. Kundens ansvar og medvirkning

Kunden skal:

- Gi nødvendige tilganger og opplysninger for at Netpower skal kunne levere tjenesten i henhold til avtalen.
- Sørge for datakvalitet i egne registreringer.
- Gi tilbakemeldinger uten ugrunnet opphold.
- Bruke applikasjonen i samsvar med formålet den er utviklet for, og i tråd med gjeldende lover, forskrifter og interne rutiner.
- Sørge for at tilgangsstyring og brukeradministrasjon ivaretas iht. prinsippet om behovsprøvd tilgang ("need-to-know"), og at uautorisert eller utilsiktet bruk av systemet ikke finner sted.
- Ikke benytte applikasjonen til andre formål enn avtalt, eller lagre informasjon som er åpenbart uegnet for systemet (f.eks. helseopplysninger dersom dette ikke er avtalt skriftlig eller regulert i databehandleravtalen mellom Partene).

Netpower er ansvarlig for å levere en sikker og stabil løsning i henhold til denne SLA og hovedavtalen. Kunden er ansvarlig for hvordan løsningen tas i bruk internt, og for eventuelle konsekvenser av feil bruk, manglende tilgangsstyring eller lagring av informasjon utover det systemet er beregnet for.

18. Ansvarsbegrensning

Ansvarsbegrensning reguleres av hovedavtalen mellom Netpower og kunden.
For tydelighet presiseres at Netpower ikke kan holdes ansvarlig for feil som skyldes kundens egne data, kundens systemer eller tredjepartsleveranser.

19. Opsjon: Vakttelefon / utvidet SLA

Mot tillegg kan kunden bestille vakttelefon.

- **Formål:** Vakttelefonen er etablert for å sikre at applikasjonen er tilgjengelig, og at driftstjenestene i Netpowers datasenter fungerer. Tjenesten gjelder kun for hendelser der applikasjonen eller servermiljøet er utilgjengelig (P1).

- **Ikke omfattet:** Vakttelefonen omfatter ikke brukerstøtte eller feilretting av funksjonalitet som kan håndteres innenfor ordinær åpningstid. Slike saker skal registreres i Zendesk og behandles i henhold til denne SLA.
- **Tilgjengelighet:** Hverdager 16:00–22:00, helg/helligdager 09:00–22:00.
- **Opsjon for 24/7:** For P1-hendelser (totalt utilgjengelig system) kan 24/7-avtale inngås særskilt.
- **Registrering:** Zendesk er alltid tilgjengelig 24/7/365 for registrering av saker.

20. Informasjonssikkerhet og ISO 27001

- Alle tjenester som omfattes av denne SLA leveres innenfor Netpowers styringssystem for informasjonssikkerhet (ISMS), som er sertifisert etter ISO/IEC 27001.
- ISMS sikrer en systematisk tilnærming til informasjonssikkerhet, inkludert styring av risiko, etablering av sikkerhetstiltak, løpende overvåkning og kontinuerlig forbedring.
- Netpower gjennomfører årlige risikovurderinger av applikasjonen, driftsmiljøet og tilhørende prosesser. I tillegg risikovurderes applikasjonen ved hver hovedrelease for å sikre at nye versjoner ikke introduserer uakseptabel risiko.
- Det utføres årlig penetrasjonstesting av Workplace Safety gjennom eksterne sikkerhetspartnere. Resultater vurderes og følges opp i tråd med ISMS.
- Kunder kan på forespørsel motta kopi av sertifikat, samt rapporter fra gjennomførte risikovurderinger og penetrasjonstester, med nødvendig hensyn til konfidensialitet.
- Sikkerhetshendelser behandles etter en definert prosess for informasjons-sikkerhetshendelser, inkludert eskalering, varsling, rotårsaksanalyse og dokumenterte korrigerende tiltak.
- Netpower stiller tilsvarende krav til underleverandører, og sikkerhet i leverandørkjeden følges opp i samsvar med ISO 27001 Annex A 5.19.
- Disaster recovery-planer og beredskapsrutiner er etablert og revideres årlig.
- Kontinuerlig forbedring av informasjonssikkerhet er en del av ISMS, og Netpower forplikter seg til å følge opp nye trusler, sårbarheter og regulatoriske krav.

21. Øvrige bestemmelser

Underleverandører, force majeure og tvisteløsning følger hovedavtalens bestemmelser.

22. Kundedriftet infrastruktur

For enkelte kunder driftes Workplace Safety på kundens egen infrastruktur eller i kundens interne datasenter. I slike tilfeller gjelder følgende særskilte bestemmelser:

- Netpower er ikke ansvarlig for fysisk sikring, redundans, strømforsyning, kjøling, overvåkning eller backup av kundens driftsmiljø. Disse forhold er kundens ansvar.
- Netpower er avhengig av at kunden gir nødvendig tilgang til miljøet for å kunne utføre oppdateringer, feilsøking eller annet arbeid. Responstider i denne SLA regnes fra tidspunktet slik tilgang er gitt.

- Netpower kan ikke garantere samme oppetid eller beredskap som i Netpowers egne datasentre, da dette er avhengig av kundens infrastruktur og rutiner.
- Kunden plikter å sikre at driftsmiljøet tilfredsstiller minimumskrav til sikkerhet og ytelse, og at Netpower får tilstrekkelig varsling og tilgang ved behov.

Dette avsnittet gjelder kun for kunder hvor driften av applikasjonen skjer på kundens egen infrastruktur eller datasenter.