TJENESTENIVÅAVTALE (SLA)

1 OMFANG OG DEFINISJONER

1.1 Denne tjenestenivåavtalen (**"SLA"**) angir de tjenestenivåene Netsecurity forplikter seg til for tjenesten Managed Detection and Response (**MDR**), og supplerer **Generelle Avtalevilkår** og **Tjenestebeskrivelsen**. Uttrykk med stor forbokstav har samme betydning som i Generelle Avtalevilkår. Ved motstrid går Tilbudet og Tjenestebeskrivelsen foran denne SLA-en, jf. Generelle Avtalevilkår punkt 1.2.

1.2 I denne SLA-en betyr:

- **SOC**: Netsecuritys sikkerhetsovervåkingssenter (Security Operations Center).
- **IRT**: Netsecuritys hendelseshåndteringsteam (Incident Response Team).
- **Kundeportal**: Netsecuritys nettbaserte portal der Kunden får innsyn i hendelser, varsler og rapporter.
- **Verifisert hendelse**: en hendelse som SOC har analysert og bekreftet som en reell sikkerhetshendelse.
- **Varsling**: melding fra Netsecurity til Kunden om en Verifisert hendelse, gitt etter den varslingsrutinen som avtales med Kunden.
- **Eskalering**: overføring av en Verifisert hendelse til riktig nivå for videre håndtering – Kunden og/eller IRT.
- **Kritikalitet**: klassifiseringen av en hendelse etter punkt 4, som avgjør hvilken responstid som gjelder.

1.3 **Språk.** Denne SLA-en foreligger på norsk og engelsk. Den engelske versjonen er en oversettelse levert for enkelhets skyld. Ved uoverensstemmelse eller tolkningstvil mellom versjonene har den norske teksten forrang, jf. Generelle Avtalevilkår punkt 16.3.

2 RESPONSTID – VARSLING OG ESKALERING AV HENDELSER

2.1 **Definisjon.** Responstiden er tiden fra SOC har bekreftet (verifisert) en hendelse til Netsecurity har varslet Kunden via avtalt varslingsrutine og eskalert hendelsen til riktig nivå for videre håndtering (Kunden og/eller IRT). Responstiden gjelder varsling og eskalering av Verifiserte hendelser. Den er **ikke** en løsnings- eller utbedringstid, og sier ikke når hendelsen er endelig lukket.

2.2 Responstiden måles 24/7/365 og gjelder per Verifisert hendelse etter kritikalitet:

Kritikalitet	Garantert responstid (varsling og eskalering)
Kritisk	30 minutter
Høy	2 timer
Middels	24 timer
Lav	48 timer
Informasjon	Kun rapportering (ingen responstidsgaranti)

Tid der Netsecurity venter på nødvendig informasjon eller handling fra Kunden, regnes ikke med.

3 RESPONSTID – HENDELSESHÅNDTERING (IRT)

3.1 **Definisjon.** IRT-responstiden er tiden fra en Verifisert hendelse eskaleres til IRT – fra SOC eller direkte fra Kunden – til IRT aktivt håndterer hendelsen ("hands-on-keyboard", dvs. at en analytiker har påbegynt konkret arbeid med hendelsen).

3.2 Følgende responstider gjelder, målt 24/7/365:

Eskaleringskilde	Responstid
Hendelser eskalert fra SOC-tjenesten	1 time
Hendelser eskalert fra Kunden	2 timer
Fysisk oppmøte hos Kunden	Etter avtale

4 KLASSIFISERING AV KRITIKALITET

4.1 Netsecuritys analyse av hendelser setter kritikalitet etter tabellen nedenfor. Kritikaliteten avgjør hvilken responstid i punkt 2 som gjelder.

4.2 Kritikalitet fastsettes ut fra Kundens miljøprofil – "Enterprise Solutions" eller "Kritisk infrastruktur" – slik denne fremgår av Tilbudet.

Hendelsestype	Enterprise Solutions	Kritisk infrastruktur
Kompromittering av høyprivilegert konto	Kritisk	Kritisk
Aktivt innbrudd	Kritisk	Kritisk
Innbrudd oppdaget	Høy	Kritisk
Informasjons-/innholdssikkerhet	Høy	Høy
Innbruddsforsøk	Middels	Høy
Tilgjengelighet	Middels	Kritisk
Kompromitterte brukere	Middels	Kritisk
Svindel	Middels	Middels
Rekognosering / informasjonsinnhenting	Lav	Middels
Mistenkelig endring	Lav	Middels
Mistenkelig brukeraktivitet	Lav	Middels
Skadelig kode blokkert av systemet	Lav	Middels
Misbruk / upassende innhold	Lav	Lav
Forbedringsområder / potensiell fremtidig risiko	Informasjon	Informasjon

5 TILGJENGELIGHET – KUNDEPORTAL

5.1 Med **tilgjengelighet** menes andelen av tjenestetiden der Kundeportalen er i drift og tilgjengelig for Kunden. Garantert tilgjengelighet for Kundeportalen er 99 % målt per kalendermåned.

5.2 Planlagt vedlikehold varslet på forhånd, og nedetid som skyldes forhold utenfor Netsecuritys kontroll eller forhold Kunden svarer for, regnes ikke som nedetid.

6 TJENESTEKREDITTER

6.1 Dersom Netsecurity ikke varsler Kunden innen garantert responstid etter punkt 2, gis Kunden en kreditt på 10 % av det samlede månedlige vederlaget for kundesupport-pakken som inngår i Tilbudet, for hvert slikt avvik i måneden.

6.2 Dersom Netsecurity ikke responderer innen garantert responstid etter punkt 3, gis Kunden en kreditt på 10 % av det samlede månedlige vederlaget for MDR-IT Base-pakken som inngår i Tilbudet, for hvert slikt avvik i måneden.

6.3 Samlet kreditt i én måned kan ikke overstige 100 % av det samlede månedlige vederlaget for pakkene i punkt 6.1 og 6.2.

6.4 Kreditten trekkes fra fakturaen for den aktuelle måneden. Retten til kreditt kommer i tillegg til øvrige rettigheter og beføyelser etter Avtalen eller gjeldende rett.

SERVICE LEVEL AGREEMENT (SLA)

1 SCOPE AND DEFINITIONS

1.1 This service level agreement (**"SLA"**) sets out the service levels Netsecurity commits to for the Managed Detection and Response (**MDR**) service, and supplements the **General Terms and Conditions** and the **Service Description**. Capitalised terms have the meaning given in the General Terms and Conditions. In the event of conflict, the Offer and the Service Description take precedence over this SLA, cf. clause 1.2 of the General Terms and Conditions.

1.2 In this SLA:

- **SOC**: Netsecurity's Security Operations Center.
- **IRT**: Netsecurity's Incident Response Team.
- **Customer Portal**: Netsecurity's web-based portal where the Customer accesses incidents, notifications and reports.
- **Verified incident**: an incident that the SOC has analysed and confirmed as a genuine security incident.
- **Notification**: a message from Netsecurity to the Customer about a Verified incident, given in accordance with the notification routine agreed with the Customer.
- **Escalation**: transfer of a Verified incident to the correct level for further handling – the Customer and/or the IRT.
- **Criticality**: the classification of an incident under clause 4, which determines the applicable response time.

1.3 **Language.** This SLA is available in Norwegian and English. The English version is a translation provided for convenience only. In the event of any discrepancy or dispute regarding interpretation between the versions, the Norwegian text shall prevail, cf. clause 16.3 of the General Terms and Conditions.

2 RESPONSE TIME – INCIDENT NOTIFICATION AND ESCALATION

2.1 **Definition.** The response time is the time from the SOC having confirmed (verified) an incident until Netsecurity has notified the Customer in accordance with the agreed notification routine and escalated the incident to the correct level for further handling (the Customer and/or the IRT). The response time covers notification and escalation of Verified incidents. It is **not** a resolution or remediation time and does not indicate when the incident is finally closed.

2.2 The response time is measured 24/7/365 and applies per Verified incident by criticality:

Criticality	Guaranteed response time (notification and escalation)
Critical	30 minutes
High	2 hours
Medium	24 hours
Low	48 hours
Information	Reporting only (no response-time guarantee)

Time during which Netsecurity is awaiting necessary information or action from the Customer is not counted.

3 RESPONSE TIME – INCIDENT MANAGEMENT (IRT)

3.1 **Definition.** The IRT response time is the time from a Verified incident being escalated to the IRT – from the SOC or directly from the Customer – until the IRT is actively handling the incident ("hands-on-keyboard", i.e. an analyst has begun concrete work on the incident).

3.2 The following response times apply, measured 24/7/365:

Escalation source	Response time
Incidents escalated from the SOC service	1 hour
Incidents escalated from the Customer	2 hours
Physical attendance at the Customer's premises	By appointment

4 CRITICALITY CLASSIFICATION

4.1 Netsecurity's analysis of events sets the criticality according to the table below. The criticality determines which response time in clause 2 applies.

4.2 Criticality is set based on the Customer's environment profile – "Enterprise Solutions" or "Critical infrastructure" – as stated in the Offer.

Type of event	Enterprise Solutions	Critical infrastructure
Compromise of high-privileged account	Critical	Critical
Active intrusion	Critical	Critical
Intrusion detected	High	Critical
Information / content security	High	High
Intrusion attempts	Medium	High
Availability	Medium	Critical
Compromised users	Medium	Critical
Fraud	Medium	Medium
Recon / information gathering	Low	Medium
Suspicious change	Low	Medium
Suspicious user activity	Low	Medium
Malicious code blocked by the system	Low	Medium
Abusive content	Low	Low
Improvement areas / potential future risks	Information	Information

5 AVAILABILITY – CUSTOMER PORTAL

5.1 **"Availability"** means the proportion of the service hours during which the Customer Portal is operational and available to the Customer. Guaranteed availability of the Customer Portal is 99 % measured per calendar month.

5.2 Planned maintenance notified in advance, and downtime caused by circumstances outside Netsecurity's control or for which the Customer is responsible, is not counted as downtime.

6 SERVICE CREDITS

6.1 If Netsecurity fails to notify the Customer within the guaranteed response time under clause 2, the Customer receives a credit of 10 % of the total monthly fee for the customer support package included in the Offer, for each such deviation in the month.

6.2 If Netsecurity fails to respond within the guaranteed response time under clause 3, the Customer receives a credit of 10 % of the total monthly fee for the MDR-IT Base package included in the Offer, for each such deviation in the month.

6.3 The total credit in any month may not exceed 100 % of the total monthly fee for the packages in clauses 6.1 and 6.2.

6.4 The credit is deducted from the invoice for the month in question. The right to a credit is in addition to any other rights and remedies under the Agreement or applicable law.