

Service Level Agreement (SLA)

NOTE: The text that follows is the German version of this document. An English translation is provided further below; every effort has been made to render the German wording as accurately as possible. (see §1.5 of this SLA)

Dieses Service Level Agreement („SLA“) ergänzt die Allgemeinen Geschäftsbedingungen („AGB“) der NeoProtect GmbH und regelt die Support-, Reaktions- und Kompensationsverpflichtungen gegenüber dem Kunden. Bei Widersprüchen zwischen diesem SLA und den AGB haben die AGB Vorrang (vgl. AGB §7.2). Fragen der Haftung richten sich ausschließlich nach den AGB.

Dieses SLA begründet eine Leistungsbeschreibung. Die hierin definierten Reaktionszeiten und Service-Level stellen Leistungsziele dar, keine Beschaffenheitsgarantie und kein selbstständiges Garantieverprechen im Sinne des § 276 BGB.

§1 Geltungsbereich

(1) Dieses SLA gilt ausschließlich für folgende Managed-Software-Produkte, die auf der Infrastruktur des Kunden betrieben werden:

- On Premise Shield
 - On Premise Business Plan
 - On Premise Enterprise Plan
- OOL (Out-of-Line) Shield

(2) Das Produkt **Game Shield** ist ausdrücklich und vollständig von diesem SLA ausgenommen. Support wird nach bestem Bemühen („best effort“) geleistet.

(3) Dieses SLA gilt ausschließlich für Kunden, die Unternehmer im Sinne des § 14 BGB sind und einen aktiven Vertrag ohne offene Zahlungsrückstände unterhalten. Verbraucher im Sinne des § 13 BGB sind vom Geltungsbereich dieses SLA ausgenommen. Weitere Voraussetzung ist ein zwischen NeoProtect und dem Kunden geschlossenes formelles Angebot, das von beiden Parteien unterzeichnet und im Zeitpunkt der Inanspruchnahme wirksam ist und in dem dieses SLA ausdrücklich in Bezug genommen wird. Fehlt ein solches Angebot, ist es nicht oder nicht mehr wirksam oder nimmt es dieses SLA nicht ausdrücklich in Bezug, so bestehen keine Ansprüche aus diesem SLA; Support wird in diesem Fall nach bestem Bemühen („best effort“) geleistet. Bei Verstoß gegen die AGB ruhen sämtliche SLA-Ansprüche.

(4) Die Produkte gemäß §1 Abs. 1 werden als verwaltete Software betrieben, die in die Kundeninfrastruktur integriert ist. Der Integrationsgrad variiert je nach Produkt: Beim On Premise Enterprise Plan ist die NeoProtect-Software tief in die Netzwerkinfrastruktur des Kunden eingebunden, während beim On Premise Business Plan und beim OOL Shield die Integration in geringerem Umfang erfolgt.

Aufgrund dieser technischen Verzahnung können Änderungen an der Kundeninfrastruktur – insbesondere bei tief integrierten Produkten – unmittelbare und unvorhersehbare Auswirkungen auf die Funktion der NeoProtect-Software haben.

Die Verpflichtungen dieses SLA beziehen sich ausschließlich auf die von NeoProtect erbrachten Leistungen: Softwarebereitstellung, -konfiguration, -wartung, Support und aktive Mitwirkung bei Vorfällen. Verfügbarkeit, Leistungsfähigkeit und Sicherheit der zugrunde liegenden Kundeninfrastruktur (Hardware, Netzwerk, Betriebssystem, Stromversorgung) liegen im alleinigen Verantwortungsbereich des Kunden. NeoProtect schuldet in Bezug auf die Kundeninfrastruktur weder Überwachung noch Beratung, es sei denn, dies ist im Angebot ausdrücklich vereinbart.

(5) Dieses SLA wird in deutscher Sprache verfasst. Die deutschsprachige Fassung ist die allein verbindliche Version. Übersetzungen dienen ausschließlich Informationszwecken.

§2 Definitionen

MRR (Monthly Recurring Revenue): Die monatlich wiederkehrende Vergütung des gesamten Kundenaccounts, ohne einmalige Gebühren oder Einrichtungskosten.

Erstreaktion (First Response): Die erste menschliche Antwort auf ein Ticket durch einen NeoProtect-Mitarbeiter, die bestätigt, dass der Vorfall zur Kenntnis genommen wurde und die Bearbeitung aufgenommen wird. Die Erstreaktion muss mindestens enthalten: Bestätigung des Eingangs, die von NeoProtect zugewiesene oder bestätigte Severity, sowie die Angabe des zuständigen Bearbeiters oder Teams. Eine inhaltliche Diagnose, Ursachenanalyse oder Lösungszusage ist nicht Bestandteil der Erstreaktion und wird nicht innerhalb der Reaktionszeit geschuldet. Automatisierte Eingangsbestätigungen gelten nicht als Erstreaktion.

On-Call Incident Response: Der Zeitraum zwischen Meldung eines kritischen Vorfalls und dem Beginn der aktiven Bearbeitung durch einen qualifizierten NeoProtect-Engineer.

Kundeninfrastruktur: Die gesamte vom Kunden bereitgestellte Hardware, Netzwerkanbindung, Stromversorgung und Betriebssystemumgebung, auf der die NeoProtect-Software betrieben wird.

NeoProtect-Software: Die von NeoProtect bereitgestellte und verwaltete DDoS-Schutzsoftware einschließlich Konfigurationen und Regelwerke.

Geschäftszeiten: Montag bis Freitag, 10:00 - 19:00 Uhr MEZ/MESZ, ausgenommen gesetzliche Feiertage am Sitz von NeoProtect.

Integrationsrelevante Infrastrukturänderung: Eine Änderung an der Kundeninfrastruktur, die nach vernünftigem Ermessen geeignet ist, die Funktion der NeoProtect-Software zu beeinträchtigen. Hierzu zählen insbesondere Änderungen an Netzwerktopologie, Routing, Firewall-Regeln, Betriebssystem, Hardware und Firmware der Systeme, auf denen oder in deren unmittelbarem Zusammenspiel die NeoProtect-Software betrieben wird. Nicht dazu zählen Änderungen, die die Funktionsfähigkeit der NeoProtect-Software offensichtlich und in

keinem Szenario beeinträchtigen können (z. B. Austausch nicht beteiligter Peripheriegeräte, Änderungen an vollständig getrennten Netzsegmenten).

SLA-Verstoß (Critical): Eine Überschreitung der in Abschnitt 5 definierten On-Call Incident Response-Zeiten durch NeoProtect, sofern die Ursache des zugrunde liegenden Vorfalls nachweislich in der NeoProtect-Software liegt und keine Ausschlüsse gemäß Abschnitt 11 greifen.

Unbegründeter On-Call-/Eskalationsabruf: Ein Abruf der On-Call Incident Response oder eine Eskalationsanforderung, bei dem oder der die jeweiligen Voraussetzungen nach Feststellung von NeoProtect nicht vorlagen. Die Bewertung erfolgt durch NeoProtect auf Basis der zum Zeitpunkt der Prüfung vorliegenden Informationen und ist für den Kunden bindend, sofern dieser nicht innerhalb von 7 Tagen nach Zugang der Rechnung schriftlich mit Begründung und Nachweisen widerspricht.

§3 MRR Stufen

Die Reaktionszeiten richten sich nach der MRR-Stufe des Kundenaccounts:

Tier	MRR
Tier 1	ab 10.000 €
Tier 2	2.000 € – 9.999 €
Tier 3	500 € – 1.999 €
Tier 4	unter 500 €

Die Zuordnung wird monatlich auf Basis der MRR des Vormonats ermittelt. Neukunden werden anhand der im Angebot vereinbarten MRR eingestuft.

§4 Severity Level

Die initiale Severity wird automatisch durch das NeoProtect-System bestimmt. Der Kunde kann die zugewiesene Severity über das Kundenportal ändern, mit Ausnahme der Severity Critical: Diese kann ausschließlich durch den Kunden über die dedizierte On-Call-Funktion (z. B. On-Call-Button im Kundenportal) ausgelöst werden und erfordert eine aktive, bewusste Handlung des Kunden. Eine automatische Einstufung als Critical durch das System erfolgt nicht.

NeoProtect behält sich vor, die Severity nach erster Analyse mit Begründung anzupassen. Die Regelungen zu unbegründeten On-Call-Abrufen gemäß Abschnitt 5 bleiben hiervon unberührt.

Critical: Mindestens 10 % des durch die NeoProtect-Software geschützten legitimen Traffics des Kunden sind nachweislich beeinträchtigt (Paketverlust, Unerreichbarkeit, erhebliche Latenzerhöhung), und die Ursache liegt in der NeoProtect-Software — nicht in der Kundeninfrastruktur. Vorfälle unterhalb dieser Schwelle sind nicht als Critical einzustufen,

unabhängig von ihrer sonstigen Auswirkung. Auslöser für On-Call Incident Response (Abschnitt 5). **Die On-Call-Funktion steht ausschließlich Kunden der MRR-Stufen Tier 1 bis Tier 3 zur Verfügung.**

High: Funktionsbeeinträchtigung der NeoProtect-Software, die unterhalb der Critical-Schwelle liegt: unvollständige Mitigation bei laufendem Angriff ohne Erreichen der 10 %-Schwelle, erhöhte Latenz durch die Software, zeitweise Einschränkungen der Schutzfunktion, fehlerhafte Anwendung einzelner Filterregeln mit messbarer Auswirkung auf den Traffic.

Medium: Nicht-dringende technische Probleme ohne unmittelbare Auswirkung auf die Schutzfunktion: fehlerhafte Regelanwendung ohne messbare Traffic-Beeinträchtigung, Konfigurationsanfragen, Anpassung von Regelwerken, Darstellungsfehler im Dashboard, Log- oder Reporting-Probleme.

Low: Alle sonstigen Anfragen, insbesondere: allgemeine Fragen zum Produkt, Feature Requests, Dokumentation, Abrechnung, Vertragsfragen, Zugangsverwaltung.

§5 On-Call Incident Response (Critical)

Für Vorfälle der Severity Critical gelten folgende Zeiten bis zum Beginn der aktiven Bearbeitung durch einen qualifizierten NeoProtect-Engineer. On-Call gilt 24/7/365.

On-Call Incident Response steht Kunden der MRR-Stufe Tier 4 nicht zur Verfügung; Critical-Vorfälle werden bei Tier 4 als High behandelt und im Rahmen der Support-Reaktionszeiten gemäß Abschnitt 6 bearbeitet.

Tier 1	Tier 2	Tier 3	Tier 4
--------	--------	--------	--------

15 min	30 min	1 h	-
--------	--------	-----	---

Der Kunde muss sicherstellen, dass NeoProtect den erforderlichen Remote-Zugang zur Software hat. Verzögerungen durch fehlenden Zugang gehen nicht zu Lasten von NeoProtect. Die Zeitmessung beginnt mit Eingang der Meldung über das Ticket-System oder den vereinbarten Kommunikationskanal und pausiert, solange NeoProtect auf eine für die Bearbeitung notwendige Rückmeldung oder Mitwirkung des Kunden wartet.

Stellt NeoProtect nach Aufnahme der Bearbeitung fest, dass ein als Critical eingestufteter Vorfall die Voraussetzungen der Severity Critical nicht erfüllt, stuft NeoProtect die Severity entsprechend herab und bearbeitet den Vorfall im Rahmen der regulären Support-Reaktionszeiten gemäß Abschnitt 6 weiter. Eine nachvollziehbare, im Zeitpunkt der Meldung vertretbare Fehleinschätzung des Kunden bleibt kostenfrei. Der On-Call-Aufwand ab Eingang der Meldung wird nur dann nach den zum Zeitpunkt der Leistungserbringung gültigen, dem Kunden zuvor bekannt gegebenen Stundensätzen in Rechnung gestellt, mindestens jedoch mit einer Pauschale von 250 € netto pro Abruf, wenn der Kunde die Critical-Meldung missbräuchlich oder grob fahrlässig ausgelöst hat. NeoProtect teilt dem Kunden die Herabstufung sowie die Gründe hierfür in Textform mit. NeoProtect kann auf die Berechnung im Einzelfall nach billigem Ermessen verzichten. Der Kunde kann innerhalb von

14 Tagen ab Zugang der Mitteilung in Textform eine Überprüfung der Einstufung und der Berechnung verlangen; NeoProtect prüft den Einwand ergebnisoffen und teilt das Ergebnis begründet mit. Bei wiederholter missbräuchlicher oder grob fahrlässiger Inanspruchnahme des On-Call (mehr als 3 Vorfälle innerhalb von 12 Monaten, die nach Prüfung durch NeoProtect herabgestuft wurden) ist NeoProtect berechtigt, den On-Call-Zugang des Kunden bis auf Weiteres zu sperren und Critical-Meldungen ausschließlich nach vorheriger Rücksprache mit einem NeoProtect-Engineer entgegenzunehmen. Gesetzliche Rechte des Kunden bleiben unberührt.

§6 Support-Reaktionszeiten (High, Medium, Low)

Für alle nicht-kritischen Anfragen gelten folgende Erstreaktionszeiten:

(1) Innerhalb der Geschäftszeiten gelten folgende Erstreaktionszeiten:

Severity	Tier 1	Tier 2	Tier 3	Tier 4
High	30 min	1 h	2 h	4 h
Medium	2 h	4 h	8 h	12 h
Low	48 h	48 h	72 h	72 h

(2) Außerhalb der Geschäftszeiten gelten folgende Erstreaktionszeiten:

Severity	Tier 1	Tier 2	Tier 3	Tier 4
High	10 h	12 h	24 h	36 h
Medium	nä. GT	nä. GT	48h	48 h
Low	48 h	48 h	72 h	72 h

nä. GT = nächster Geschäftstag. Medium- und Low-Tickets außerhalb der Geschäftszeiten werden am folgenden Geschäftstag bearbeitet.

Maßgeblich für die anwendbare Reaktionszeit ist, ob der Zeitpunkt der Ticketerstellung zuzüglich der jeweiligen Reaktionszeit noch vollständig innerhalb der laufenden Geschäftszeiten liegt. Ist dies der Fall, gelten die Reaktionszeiten gemäß §6 Abs. 1. Andernfalls gelten die Reaktionszeiten gemäß §6 Abs. 2. Der Zeitpunkt der Ticketerstellung bestimmt sich nach dem im Ticket-System von NeoProtect dokumentierten Eingangszeitstempel.

(3) Die Reaktionszeit beginnt mit der Erstellung des Tickets. Fordert NeoProtect — gleich ob durch automatisierte Systeme oder durch einen Mitarbeiter — den Kunden zur Bereitstellung von Informationen, Zugangsdaten, Logs oder sonstiger Mitwirkung auf, endet die laufende Zeitmessung. Mit Eingang der vollständigen Kundenantwort beginnt die Reaktionszeit erneut von Beginn an. Unvollständige oder nicht verwertbare Antworten lösen keinen Neubeginn der Zeitmessung aus.

Maßgeblich für die anwendbare Reaktionszeit (§6 Abs. 1 oder 6.2) ist jeweils der Zeitpunkt des Neubeginns der Zeitmessung. Liegt dieser Zeitpunkt zuzüglich der jeweiligen Reaktionszeit noch vollständig innerhalb der laufenden Geschäftszeiten, gelten die Reaktionszeiten gemäß §6 Abs. 1, andernfalls §6 Abs. 2.

Stellt der Kunde die angeforderten Informationen nicht innerhalb von 72 Stunden bereit, ist NeoProtect berechtigt, die Severity des Tickets auf Low herabzustufen. Bleibt die angeforderte Mitwirkung auch nach angemessener Frist aus, kann NeoProtect das Ticket ohne weitere Ankündigung schließen. Was als angemessen gilt, richtet sich nach der Severity des Vorfalls und der Art der angeforderten Information. Ein geschlossenes Ticket begründet keinen SLA-Verstoß.

Alle Zeitstempel werden durch das Ticket-System von NeoProtect dokumentiert und sind für die Berechnung der Reaktionszeiten maßgeblich.

§7 Eskalation

Eine Eskalation erfolgt ausschließlich über die On-Call-Funktion gemäß Abschnitt 5 und setzt voraus, dass der Kunde den Vorfall als Critical einstuft. Ein separater Eskalationsmechanismus besteht nicht. Es gelten dieselben Voraussetzungen, Kosten und Konsequenzen wie bei einem regulären On-Call-Abruf. Kunden der MRR-Stufe Tier 4 steht keine Eskalationsmöglichkeit zur Verfügung.

§8 Mitwirkungspflichten des Kunden

Der Kunde ist verpflichtet:

- (a) NeoProtect dauerhaften Remote-Zugang zur NeoProtect-Software bereitzustellen.
- (b) Einen technischen Ansprechpartner zu benennen, der bei Critical-Vorfällen innerhalb von 30 Minuten erreichbar ist.
- (c) Integrationsrelevante Infrastrukturänderungen im Sinne von Abschnitt 2 mindestens 48 Stunden im Voraus schriftlich anzukündigen.
- (d) Bei der Geltendmachung von SLA-Credits die erforderlichen Nachweise (Ticket-Nummern, Zeitstempel, Vorfallbeschreibung) beizubringen.

Kommt der Kunde seinen Mitwirkungspflichten nicht nach, stellt eine daraus resultierende Verzögerung keinen SLA-Verstoß dar. Insbesondere kann sich der Kunde nicht auf Fristüberschreitungen berufen, wenn diese durch seine fehlende oder verspätete Mitwirkung verursacht oder mitverursacht wurden.

§9 Suspension bei Infrastrukturänderungen

(1) Dieser Abschnitt gilt ausschließlich für integrationsrelevante Infrastrukturänderungen im Sinne von Abschnitt 2. Änderungen an der Kundeninfrastruktur, die die Funktionsfähigkeit der NeoProtect-Software offensichtlich nicht beeinträchtigen können, lösen keine Suspension aus.

(2) Nimmt der Kunde eine integrationsrelevante Infrastrukturänderung vor — gleich ob angekündigt oder unangekündigt — so ruhen sämtliche Verpflichtungen aus diesem SLA ab dem Zeitpunkt der Änderung.

Die Suspension gilt, bis NeoProtect die ordnungsgemäße Funktion der NeoProtect-Software in der veränderten Umgebung geprüft und schriftlich bestätigt hat. NeoProtect ist nicht verpflichtet, diese Prüfung innerhalb eines bestimmten Zeitraums durchzuführen. NeoProtect wird die Prüfung jedoch ohne unangemessene Verzögerung nach Kenntniserlangung durchführen.

(3) Der Aufwand für Prüfung und etwaige Anpassungen kann dem Kunden gesondert in Rechnung gestellt werden, sofern die Änderung ohne vorherige Abstimmung mit NeoProtect gemäß Abschnitt 8(c) erfolgte. Die Abrechnung erfolgt nach den zum Zeitpunkt der Leistungserbringung gültigen Stundensätzen von NeoProtect.

(4) Aufgrund der tieferen Netzwerkintegration beim On Premise Enterprise Plan ist der Kreis der integrationsrelevanten Änderungen bei diesem Produkt typischerweise größer als beim On Premise Business Plan oder beim OOL Shield. NeoProtect stellt dem Kunden auf Anfrage eine produktspezifische Übersicht bereit, welche Arten von Infrastrukturänderungen als integrationsrelevant eingestuft werden.

(5) Für die Dauer der Suspension bestehen keine Ansprüche auf SLA-Credits oder sonstige Kompensation.

§10 SLA-Credits

(1) SLA-Credits stellen eine pauschalierte Minderung der Vergütung dar. Sie sind kein Anerkenntnis einer Pflichtverletzung und kein Schadensersatz. Die Gewährung von SLA-Credits lässt Ansprüche des Kunden aus den AGB unberührt; bereits gewährte Credits werden jedoch auf etwaige weitergehende Ansprüche des Kunden aus demselben Vorfall angerechnet.

(2) Der Kunde hat Anspruch auf Credits, wenn NeoProtect die in Abschnitt 5 oder 6 definierten Reaktionszeiten nicht einhält. Maßgeblich ist allein, ob die Einhaltung der Reaktionszeit im Verantwortungsbereich von NeoProtect lag; auf die technische Ursache des zugrunde liegenden Vorfalls kommt es nicht an. Auch bei kundenseitig verursachten Vorfällen schuldet NeoProtect die zugesagte Reaktion. Die in Abschnitt 11 genannten Ausschlüsse greifen nur, soweit der jeweilige Umstand die Verspätung tatsächlich verursacht hat.

(3)

Überschreitung der Reaktionszeit	Credit pro Vorfall
bis 2x der vereinbarten Zeit	5 % der Monats-MRR
2x bis 4x der vereinbarten Zeit	10 % der Monats-MRR

über 4x der vereinbarten Zeit

15 % der Monats-MRR

(4) Die Summe aller Credits ist auf 30 % der monatlichen MRR pro Kalendermonat begrenzt. Credits müssen innerhalb von 30 Tagen nach dem Vorfall schriftlich unter Beifügung der in Abschnitt 8(d) genannten Nachweise geltend gemacht werden und werden mit der nächsten Rechnung verrechnet. Eine Auszahlung erfolgt nicht. Bei unvollständigen Nachweisen setzt NeoProtect dem Kunden eine angemessene Nachfrist.

(5) Treten innerhalb eines Quartals mehr als 3 SLA-Verstöße (Critical) im Sinne von Abschnitt 2 auf, erhält der Kunde ein Sonderkündigungsrecht mit 14 Tagen Frist zum Monatsende. **Für Kunden der MRR-Stufe Tier 4 bemisst sich das Sonderkündigungsrecht nach wiederholten Verstößen gegen die Support-Reaktionszeiten der Severity High, jedoch mit einem Schwellwert von 6 Verstößen innerhalb eines Quartals.**

(6) SLA-Credits sind pauschale, der Höhe nach feste Vergütungsminderungen (Preisnachlässe) für die Nichteinhaltung der zugesagten Reaktionszeiten; sie setzen kein Verschulden und keinen Schadensnachweis voraus. Ein Nachweis eines höheren oder geringeren Schadens ist für die Höhe des Credits nicht erforderlich und ändert diese nicht. Weitergehende gesetzliche oder in den AGB geregelte Ansprüche des Kunden, insbesondere Schadensersatzansprüche, bleiben von diesem Abschnitt unberührt; bereits gewährte Credits werden auf solche weitergehenden Ansprüche angerechnet, soweit sie denselben Zeitraum und dieselbe Pflichtverletzung betreffen.

(7) NeoProtect ist berechtigt, dem Kunden Credits auf Grundlage der eigenen System- und Ticketdaten auch ohne vorherige Geltendmachung von sich aus gutzuschreiben. Eine Verpflichtung hierzu besteht nicht. Eine freiwillige Gutschrift stellt weder ein Anerkenntnis dem Grunde oder der Höhe nach dar noch begründet sie einen Anspruch des Kunden auf künftige automatische Gutschriften; das Erfordernis der fristgerechten Geltendmachung nach Absatz (4) bleibt für alle übrigen Fälle unberührt.

§11 Ausschlüsse

Dieses SLA findet keine Anwendung bei:

(a) Beeinträchtigungen, deren Ursache in der Kundeninfrastruktur liegt (Hardware, Netzwerk, Strom, Betriebssystem, unzureichende Kapazität).

(b) Angriffen, deren Volumen die Kapazität der Kundeninfrastruktur übersteigt und die nicht durch Softwarekonfiguration allein mitigiert werden können.

(c) Integrationsrelevanten Infrastrukturänderungen — es gelten die Regelungen in Abschnitt 9.

(d) Änderungen, die der Kunde ohne Abstimmung mit NeoProtect an der NeoProtect-Software vorgenommen hat.

- (e) Wartungsarbeiten und Updates an der NeoProtect-Software, die vom Kunden angefragt oder freigegeben wurden.
- (f) Ausfällen bei Drittanbietern, Transit-Providern oder Peering-Partnern des Kunden.
- (g) Höherer Gewalt im Sinne der AGB, einschließlich — ohne Beschränkung hierauf — staatlicher Anordnungen, großflächiger Internetausfälle, Naturkatastrophen und Pandemien.
- (h) Verstößen des Kunden gegen AUP (sofern vorhanden) oder AGB.
- (i) Fehlender oder verspäteter Mitwirkung des Kunden gemäß Abschnitt 8.
- (j) Einsatz der Software auf Infrastruktur, die nicht den von NeoProtect kommunizierten Mindestanforderungen entspricht.
- (k) DDoS-Angriffen oder sonstigen Cyberangriffen auf die Kundeninfrastruktur, die Auswirkungen auf die Erreichbarkeit der NeoProtect-Software haben, deren Ursache jedoch nicht in der NeoProtect-Software liegt.
- (l) Vorübergehende Unerreichbarkeit der Support-Systeme von NeoProtect (insbesondere das Ticketsystem im Panel oder die Support-E-Mail).

Abweichend von Buchstabe (l) und ergänzend zu den Regelungen über die Meldewege gilt: Sind die regulären Support-Systeme von NeoProtect (insbesondere das Ticketsystem im Panel oder die Support-E-Mail) vorübergehend nicht erreichbar, kann der Kunde einen Critical-Vorfall über den durchgehend (24/7) verfügbaren Ausweichkanal per E-Mail an info@neoprotect.net melden. Die Meldung gilt in diesem Fall zu dem vom Kunden nachgewiesenen Zeitpunkt seines ersten Meldeversuchs über einen der vereinbarten Kommunikationskanäle als bei NeoProtect eingegangen; die Reaktionszeit beginnt zu diesem Zeitpunkt. Eine Unerreichbarkeit der Support-Systeme von NeoProtect lässt die SLA-Verpflichtungen und die Credit-Ansprüche des Kunden unberührt und setzt insbesondere nicht die Reaktionszeit außer Kraft.

§12 Keine Lösungs- und Erfolgsgarantie

NeoProtect gibt keine Garantie auf die Lösung eines Problems innerhalb eines bestimmten Zeitraums und schuldet keine vollständige Abwehr jedes DDoS-Angriffs. Die Verpflichtungen dieses SLA beziehen sich auf Reaktion, aktive Bearbeitung und Eskalation — nicht auf ein bestimmtes Ergebnis oder eine bestimmte Mitigationsleistung. Art, Umfang und Erfolg der Mitigation hängen von einer Vielzahl von Faktoren ab, die teilweise außerhalb des Einflussbereichs von NeoProtect liegen, darunter Art und Komplexität des Angriffs, Kapazität und Konfiguration der Kundeninfrastruktur sowie die Mitwirkung des Kunden. Dies gilt in besonderem Maße nach integrationsrelevanten Änderungen an der Kundeninfrastruktur.

§13 Änderungen

NeoProtect kann dieses SLA mit einer Ankündigungsfrist von mindestens 30 Tagen in Textform ändern, sofern hierfür ein sachlicher Grund besteht (insbesondere Änderungen der Rechtslage, sicherheits- oder betriebstechnische Anforderungen, Änderungen bei

Vorleisten oder eingesetzten Technologien) und die Änderung den Kunden nicht unangemessen benachteiligt. Änderungen, die über nicht wesentliche betriebliche Anpassungen hinausgehen und das Leistungsniveau zum Nachteil des Kunden verändern, werden nur zum Beginn eines neuen Abrechnungszeitraums oder mit Zustimmung des Kunden wirksam. NeoProtect gibt die geänderte Fassung unter Angabe der geänderten Bestimmungen, der Versionsbezeichnung und des Inkrafttretensdatums bekannt. Wesentliche Verschlechterungen berechtigen den Kunden zur Sonderkündigung mit Wirkung zum Inkrafttreten der Änderung, die er innerhalb von 30 Tagen nach Bekanntgabe erklären kann; bis zum Wirksamwerden der Kündigung gelten die bisherigen Bedingungen fort. Als wesentliche Verschlechterung gelten insbesondere: Verlängerung der Reaktionszeiten um mehr als 20 %, Reduzierung der Credit-Sätze oder Einschränkung des Geltungsbereichs. Die vorstehende Regelung gilt vorbehaltlich abweichender oder zwingender Bestimmungen der AGB und des anwendbaren Rechts; die Rechte von Verbrauchern bleiben unberührt.

§14 Inkrafttreten

Dieses SLA tritt mit Abschluss eines Angebots für ein eingeschlossenes Produkt in Kraft und gilt für die Dauer des Vertragsverhältnisses.

Service Level Agreement (SLA)

NOTE: This is the English translation of the German version above. It has been prepared with the great care and tries to follow the German wording as close as possible. (see §1.5 of this SLA)

This Service Level Agreement ("SLA") supplements the General Terms and Conditions ("GTC") of NeoProtect GmbH and governs the support, response, and compensation obligations towards the customer. In the event of conflicts between this SLA and the GTC, the GTC prevail (cf. GTC §7.2). Questions of liability are governed exclusively by the GTC.

This SLA constitutes a description of services. The response times and service levels defined herein represent performance targets, not a warranty of quality and not an independent guarantee within the meaning of § 276 BGB (German Civil Code).

§1 Scope

(1) This SLA applies exclusively to the following managed software products operated on the customer's infrastructure:

- On Premise Shield
 - On Premise Business Plan
 - On Premise Enterprise Plan
- OOL (Out-of-Line) Shield

(2) The product **Game Shield** is expressly and entirely excluded from this SLA. Support is provided on a best-effort basis ("best effort").

(3) This SLA applies exclusively to customers who are entrepreneurs within the meaning of § 14 BGB and maintain an active contract without outstanding payment arrears. Consumers within the meaning of § 13 BGB are excluded from the scope of this SLA. A further prerequisite is a formal offer concluded between NeoProtect and the customer which has been signed by both parties, is effective at the time the services are claimed, and expressly references this SLA. If no such offer exists, if it is not or no longer effective, or if it does not expressly reference this SLA, no claims arise under this SLA; in such case, support is provided on a best-effort basis ("best effort"). In the event of a breach of the GTC, all SLA claims are suspended.

(4) The products pursuant to §1(1) are operated as managed software integrated into the customer infrastructure. The degree of integration varies by product: with the On Premise Enterprise Plan, the NeoProtect software is deeply embedded in the customer's network infrastructure, whereas with the On Premise Business Plan and the OOL Shield the integration occurs to a lesser extent.

Due to this technical interlocking, changes to the customer infrastructure – particularly with deeply integrated products – may have immediate and unforeseeable effects on the functioning of the NeoProtect software.

The obligations under this SLA relate exclusively to the services provided by NeoProtect: software provision, configuration, maintenance, support, and active cooperation during incidents. The availability, performance, and security of the underlying customer infrastructure (hardware, network, operating system, power supply) fall within the sole responsibility of the customer. NeoProtect owes neither monitoring nor consulting with respect to the customer infrastructure unless expressly agreed in the Offer.

(5) This SLA is drawn up in the German language. The German-language version is the sole binding version. Translations serve informational purposes only.

§2 Definitions

MRR (Monthly Recurring Revenue): The monthly recurring remuneration of the entire customer account, excluding one-time fees or setup costs.

First Response: The first human reply to a ticket by a NeoProtect employee, confirming that the incident has been acknowledged and that processing has begun. The first response must contain at least: confirmation of receipt, the severity assigned or confirmed by NeoProtect, and the designation of the responsible handler or team. A substantive diagnosis, root-cause analysis, or solution commitment is not part of the first response and is not owed within the response time. Automated acknowledgments of receipt do not qualify as a first response.

On-Call Incident Response: The period between the report of a critical incident and the start of active processing by a qualified NeoProtect engineer.

Customer Infrastructure: The entire hardware, network connectivity, power supply, and operating-system environment provided by the customer on which the NeoProtect software is operated.

NeoProtect Software: The DDoS protection software provided and managed by NeoProtect, including configurations and rule sets.

Business Hours: Monday to Friday, 10:00 – 19:00 CET/CEST, excluding public holidays at NeoProtect's registered seat.

Integration-Relevant Infrastructure Change: A change to the customer infrastructure that, upon reasonable assessment, is capable of impairing the functioning of the NeoProtect software. This includes in particular changes to network topology, routing, firewall rules, operating system, hardware, and firmware of the systems on which, or in whose immediate interaction, the NeoProtect software is operated. It does not include changes that obviously and under no scenario can impair the functionality of the NeoProtect software (e.g. replacement of unrelated peripheral devices, changes to fully separated network segments).

SLA Breach (Critical): An exceedance of the On-Call Incident Response times defined in Section 5 by NeoProtect, provided that the cause of the underlying incident demonstrably lies in the NeoProtect software and no exclusions pursuant to Section 11 apply.

Unjustified On-Call / Escalation Request: A request for On-Call Incident Response or an escalation request for which the respective prerequisites, as determined by NeoProtect, were not met. The assessment is made by NeoProtect on the basis of the information available at the time of review and is binding on the customer unless the customer objects in writing, with reasons and evidence, within 7 days of receipt of the invoice.

§3 MRR Tiers

Response times are based on the MRR tier of the customer account:

Tier	MRR
Tier 1	as of 10.000 €
Tier 2	2.000 € – 9.999 €
Tier 3	500 € – 1.999 €
Tier 4	below 500 €

The assignment is determined monthly on the basis of the previous month's MRR. New customers are classified according to the MRR agreed in the offer.

§4 Severity Levels

The initial severity is determined automatically by the NeoProtect system. The customer can change the assigned severity via the customer portal, with the exception of the Critical severity: this can only be triggered by the customer via the dedicated on-call function (e.g. on-call button in the customer portal) and requires an active, deliberate action by the customer. The system does not perform automatic classification as Critical.

NeoProtect reserves the right to adjust the severity, with reasons, after an initial analysis. The provisions on unjustified on-call requests pursuant to Section 5 remain unaffected.

Critical: At least 10% of the customer's legitimate traffic protected by the NeoProtect software is demonstrably impaired (packet loss, unreachability, significant latency increase), and the cause lies in the NeoProtect software — not in the customer infrastructure. Incidents below this threshold are not to be classified as Critical, regardless of their other impact. Trigger for On-Call Incident Response (Section 5). **The on-call function is available exclusively to customers of MRR tiers Tier 1 to Tier 3.**

High: Functional impairment of the NeoProtect software below the Critical threshold: incomplete mitigation during an ongoing attack without reaching the 10% threshold, increased latency caused by the software, temporary limitations of the protection function, faulty application of individual filter rules with a measurable effect on traffic.

Medium: Non-urgent technical problems without immediate effect on the protection function: faulty rule application without measurable traffic impairment, configuration requests, adjustment of rule sets, display errors in the dashboard, log or reporting issues.

Low: All other requests, in particular: general questions about the product, feature requests, documentation, billing, contract questions, access management.

§5 On-Call Incident Response (Critical)

For incidents of severity Critical, the following times apply until the start of active processing by a qualified NeoProtect engineer. On-call applies 24/7/365.

On-Call Incident Response is not available to customers of MRR tier Tier 4; Critical incidents for Tier 4 are treated as High and handled within the support response times pursuant to Section 6.

Tier 1	Tier 2	Tier 3	Tier 4
--------	--------	--------	--------

15 min	30 min	1 h	-
--------	--------	-----	---

The customer must ensure that NeoProtect has the necessary remote access to the software. Delays due to lack of access are not to the detriment of NeoProtect. Time measurement begins upon receipt of the report via the ticket system or the agreed communication channel and pauses for as long as NeoProtect is waiting for a response or cooperation from the customer necessary for processing.

If, after commencing processing, NeoProtect determines that an incident classified as Critical does not meet the prerequisites of the Critical severity, NeoProtect downgrades the severity accordingly and continues to handle the incident within the regular support response times pursuant to Section 6. A comprehensible misassessment by the customer that was reasonable at the time of the report remains free of charge and sanctions. The on-call effort from receipt of the report is invoiced according to the hourly rates valid at the time of performance and previously disclosed to the customer, but at least a flat fee of €250 net per request, only if the customer triggered the Critical report abusively or with gross negligence. NeoProtect notifies the customer of the downgrade and the reasons for it in text form. NeoProtect may, at its reasonable discretion, waive the charge in an individual case. Within 14 days of receipt of the notification, the customer may request, in text form, a review of the classification and the charge; NeoProtect examines the objection with an open outcome and communicates the result with reasons. In the event of repeated abusive or grossly negligent use of the on-call function (more than 3 incidents within 12 months that were downgraded after review by NeoProtect), NeoProtect is entitled to suspend the customer's on-call access until further notice and to accept Critical reports only after prior consultation with a NeoProtect engineer. The customer's statutory rights remain unaffected.

§6 Support Response Times (High, Medium, Low)

For all non-critical requests, the following first-response times apply:

(1) Within business hours, the following first-response times apply:

Severity	Tier 1	Tier 2	Tier 3	Tier 4
----------	--------	--------	--------	--------

High	30 min	1 h	2 h	4 h
Medium	2 h	4 h	8 h	12 h
Low	48 h	48 h	72 h	72 h

(2) Outside business hours, the following first-response times apply:

Severity	Tier 1	Tier 2	Tier 3	Tier 4
High	10 h	12 h	24 h	36 h
Medium	next BD	next BD	48h	48 h
Low	48 h	48 h	72 h	72 h

next BD = next business day. Medium and Low tickets outside business hours are handled on the following business day.

The applicable response time depends on whether the time of ticket creation plus the respective response time still falls entirely within the ongoing business hours. If this is the case, the response times pursuant to §6(1) apply. Otherwise, the response times pursuant to §6(2) apply. The time of ticket creation is determined by the receipt timestamp documented in NeoProtect's ticket system.

(3) The response time begins with the creation of the ticket. If NeoProtect — whether through automated systems or through an employee — requests the customer to provide information, access credentials, logs, or other cooperation, the ongoing time measurement ends. Upon receipt of the complete customer response, the response time begins anew from the start. Incomplete or unusable responses do not trigger a restart of the time measurement.

Decisive for the applicable response time (§6(1) or 6.2) is, in each case, the time of the restart of the time measurement. If this time plus the respective response time still falls entirely within the ongoing business hours, the response times pursuant to §6(1) apply, otherwise §6(2).

If the customer does not provide the requested information within 72 hours, NeoProtect is entitled to downgrade the ticket's severity to Low. If the requested cooperation remains absent even after a reasonable period, NeoProtect may close the ticket without further notice. What is considered reasonable depends on the severity of the incident and the nature of the requested information. A closed ticket does not constitute an SLA breach.

All timestamps are documented by NeoProtect's ticket system and are decisive for the calculation of the response times.

§7 Escalation

An escalation occurs exclusively via the on-call function pursuant to Section 5 and requires the customer to classify the incident as Critical. There is no separate escalation mechanism. The same prerequisites, costs, and consequences apply as for a regular on-call request. Customers of MRR tier Tier 4 have no escalation option available.

§8 Customer Cooperation Obligations

The customer is obliged:

- (a) to provide NeoProtect with permanent remote access to the NeoProtect software.
- (b) to designate a technical contact who is reachable within 30 minutes in the event of Critical incidents.
- (c) to announce integration-relevant infrastructure changes within the meaning of Section 2 in writing at least 48 hours in advance.
- (d) when asserting SLA credits, to provide the required evidence (ticket numbers, timestamps, incident description).

If the customer fails to meet its cooperation obligations, any resulting delay does not constitute an SLA breach. In particular, the customer cannot rely on time exceedances if these were caused or contributed to by its missing or delayed cooperation.

§9 Suspension upon Infrastructure Changes

- (1) This Section applies exclusively to integration-relevant infrastructure changes within the meaning of Section 2. Changes to the customer infrastructure that obviously cannot impair the functionality of the NeoProtect software do not trigger a suspension.
- (2) If the customer makes an integration-relevant infrastructure change — whether announced or unannounced — all obligations under this SLA are suspended as of the time of the change.

The suspension applies until NeoProtect has verified and confirmed in writing the proper functioning of the NeoProtect software in the changed environment. NeoProtect is not obliged to carry out this review within a specific period. However, NeoProtect will carry out the review without undue delay after becoming aware of the change.

- (3) The effort for review and any adjustments may be invoiced to the customer separately, provided that the change was made without prior coordination with NeoProtect pursuant to Section 8(c). Invoicing is based on NeoProtect's hourly rates valid at the time of performance.
- (4) Due to the deeper network integration with the On Premise Enterprise Plan, the range of integration-relevant changes for this product is typically larger than for the On Premise Business Plan or the OOL Shield. Upon request, NeoProtect provides the customer with a

product-specific overview of which types of infrastructure changes are classified as integration-relevant.

(5) For the duration of the suspension, there are no claims to SLA credits or other compensation.

§10 SLA Credits

(1) SLA credits constitute a lump-sum reduction of the remuneration. They are not an acknowledgment of a breach of duty and not damages. The granting of SLA credits leaves the customer's claims under the GTC unaffected; however, credits already granted are offset against any further claims of the customer arising from the same incident.

(2) The customer is entitled to credits if NeoProtect fails to meet the response times defined in Section 5 or 6. The decisive factor is solely whether meeting the response time lay within NeoProtect's area of responsibility; the technical root cause of the underlying incident is irrelevant. NeoProtect owes the promised response even for customer-caused incidents. The exclusions set out in Section 11 apply only to the extent that the respective circumstance actually caused the delay.

(3)

Exceedance of the Response Time	Credit per Incident
up to 2x the agreed time	5% of monthly MRR
2x to 4x the agreed time	10% of monthly MRR
over 4x the agreed time	15% of monthly MRR

(4) The sum of all credits is limited to 30% of the monthly MRR per calendar month. Credits must be asserted in writing within 30 days of the incident, together with the evidence specified in Section 8(d), and are set off against the next invoice. No payout is made. In the case of incomplete evidence, NeoProtect grants the customer a reasonable grace period.

(5) If more than 3 SLA breaches (Critical) within the meaning of Section 2 occur within a quarter, the customer receives a special termination right with 14 days' notice to the end of the month. **For customers of MRR tier Tier 4, the special termination right is measured by repeated breaches of the support response times of severity High, but with a threshold of 6 breaches within a quarter.**

(6) SLA credits are lump-sum, fixed-amount reductions in remuneration (price reductions) for failure to meet the promised response times; they require neither fault nor proof of damage. Proof of higher or lower damage is not required for the amount of the credit and does not change it. Further statutory claims or claims governed by the GTC, in particular claims for damages, remain unaffected by this Section; credits already granted are offset against such further claims to the extent they concern the same period and the same breach of duty.

(7) NeoProtect is entitled to credit the customer on the basis of its own system and ticket data on its own initiative, even without prior assertion. There is no obligation to do so. A voluntary credit constitutes neither an acknowledgment as to cause or amount nor does it establish a claim of the customer to future automatic credits; the requirement of timely assertion pursuant to paragraph (4) remains unaffected for all other cases.

§11 Exclusions

This SLA does not apply in the case of:

- (a) impairments whose cause lies in the customer infrastructure (hardware, network, power, operating system, insufficient capacity).
- (b) attacks whose volume exceeds the capacity of the customer infrastructure and which cannot be mitigated by software configuration alone.
- (c) integration-relevant infrastructure changes — the provisions in Section 9 apply.
- (d) changes that the customer has made to the NeoProtect software without coordination with NeoProtect.
- (e) maintenance work and updates to the NeoProtect software that were requested or approved by the customer.
- (f) outages at third-party providers, transit providers, or peering partners of the customer.
- (g) force majeure within the meaning of the GTC, including — without limitation — governmental orders, large-scale internet outages, natural disasters, and pandemics.
- (h) breaches by the customer of the AUP (if any) or the GTC.
- (i) missing or delayed cooperation by the customer pursuant to Section 8.
- (j) use of the software on infrastructure that does not meet the minimum requirements communicated by NeoProtect.
- (k) DDoS attacks or other cyberattacks on the customer infrastructure that affect the reachability of the NeoProtect software but whose cause does not lie in the NeoProtect software.
- (l) temporary unavailability of NeoProtect's support systems (in particular the ticket system in the panel or the support email).

Notwithstanding point (l) and in addition to the provisions on reporting channels, the following applies: if NeoProtect's regular support systems (in particular the ticket system in the panel or the support email) are temporarily unavailable, the customer may report a Critical incident via the continuously (24/7) available backup channel by email to info@neoprotect.net. In this case, the report is deemed received by NeoProtect at the time, evidenced by the customer, of its first reporting attempt via one of the agreed communication channels; the response time starts at that point. Unavailability of NeoProtect's support

systems does not affect the SLA obligations and the customer's credit claims and, in particular, does not suspend the response time.

§12 No Solution or Success Guarantee

NeoProtect gives no guarantee for the solution of a problem within a specific period and does not owe complete mitigation of every DDoS attack. The obligations under this SLA relate to response, active processing, and escalation — not to a specific result or a specific mitigation performance. The nature, extent, and success of the mitigation depend on a variety of factors, some of which lie outside NeoProtect's sphere of influence, including the type and complexity of the attack, the capacity and configuration of the customer infrastructure, and the customer's cooperation. This applies in particular after integration-relevant changes to the customer infrastructure.

§13 Changes

NeoProtect may change this SLA with at least 30 days' notice in text form, provided there is an objective reason for doing so (in particular changes in the legal situation, security-related or operational requirements, changes at upstream providers or in the technologies used) and the change does not unreasonably disadvantage the customer. Changes that go beyond non-material operational adjustments and alter the service level to the customer's detriment take effect only at the start of a new billing period or with the customer's consent. NeoProtect announces the amended version, stating the amended provisions, the version designation and the effective date. Material deteriorations entitle the customer to special termination effective as of the date the change takes effect, which the customer may declare within 30 days of notification; until the termination takes effect, the previous conditions continue to apply. Material deteriorations include in particular: extension of response times by more than 20%, reduction of credit rates, or restriction of the scope. The foregoing applies subject to any diverging or mandatory provisions of the GTC and applicable law; the rights of consumers remain unaffected.

§14 Entry into Force

This SLA enters into force upon the conclusion of an offer for an included product and applies for the duration of the contractual relationship.