



# SecureCall – Deutsch

## Technical Security Services

<b>Name</b>	Leistungsbeschreibung: SecureCall – Deutsch
<b>Owner</b>	TSS Management
<b>Status</b>	APPROVED
<b>Classification</b>	CONFIDENTIAL-EXTERNAL
<b>Version</b>	V6.0
<b>Date</b>	29 June 2018
<b>Review</b>	30 June 2018

## Inhalt

### Leistungsbeschreibung: SecureCall – Deutsch

<b>1 Einleitung</b>	<b>3</b>
1.1 Zweck des Dokuments	3
1.2 Dokumentenstruktur Supportvertrag	3
1.3 Begriffsbestimmungen	3
<b>2. Service</b>	<b>4</b>
2.1 Servicelevel	4
2.2 Umfang des Support Service	4
<b>3 Kenndaten der Support Services</b>	<b>4</b>
3.1 Ein Ansprechpartner (Single Point of Contact)	4
3.2 Sprachunterstützung	4
3.3 Technischer Support	4
3.4 Hardware Support – einschließlich RMA	4
3.5 Management von Supportanfragen	4
• 3.5.1 Bearbeitung von Supportanfragen	4
• 3.5.2 Einreichen/Generieren von Supportanfragen	5
• 3.5.3 Erste Reaktion Servicelevel	5
• 3.5.4 Fehlerbehebung über Fernzugriff	5
• 3.5.5 Überwachung von Supportanfragen	5
• 3.5.6 Eskalation von Supportanfragen	6
• 3.5.7 Abschluss von Supportanfragen – Ursachenanalyse	6
3.6 Best Practices für Update und Upgrade	6
3.7 Zugang zum Online-Portal von SecureCall	6
3.8 Support Update Service (SUS)	6
3.9 Vor-Ort-Unterstützung (kostenpflichtige Option)	7
3.10 Technischer Account-Manager (kostenpflichtige Option)	7
3.11 SecureHands – Technische Unterstützung per Fernzugriff (kostenpflichtige Option)	7
• 3.11.1 SecureHands-Leistungszeiten und Sprachen	8
• 3.11.2 Beschaffung und SecureHands-Einheitenmanagement	8
• 3.11.3 Stornierung einer SecureHands-Sitzung	8
• 3.11.4 Management von SecureHands Supportanfragen	9
• 3.11.5 SecureHands Servicelevel-Ziele	9
• 3.11.6 Abschluss und Annahme von SecureHands-Sitzungen	9
• 3.11.7 SecureHands-Servicegutschriften	9
3.12 Bewertung der Technologiebasis (kostenpflichtige Option)	9
• 3.12.1 Übersicht der Service-Optionen	9
3.13 Schwachstellenanalyse (kostenpflichtige Option)	10
• 3.13.1 Schwachstellenanalyse	10
• 3.13.2 Anforderung von Schwachstellenanalysen	10
• 3.13.3 Zielsetzung einer Schwachstellenanalyse	10
<b>4 Sicherheitstechnik-Training (STT)</b>	<b>10</b>
4.1 Kursbeschreibung	10
<b>5 Verantwortlichkeiten</b>	<b>10</b>
5.1 Verantwortlichkeiten des Kunden	10
• 5.1.1 Allgemeine Verantwortlichkeiten des Kunden	10
• 5.1.2 Fehlerbehebung im Fernzugriff und SecureHands	11
5.2 Verantwortlichkeiten von NTT Ltd.	12
• 5.2.1 Allgemeine Verantwortlichkeiten von NTT Ltd.	12

## 1 Einleitung

### 1.1 Zweck des Dokuments

Diese Beschreibung des Support Services ist Teil des Supportvertrags von NTT Ltd. mit dem Kunden. Sie beschreibt die Funktionen des Service SecureCall, erklärt, wie Supportanfragen je nach Priorität verarbeitet werden, und legt den Eskalationsprozess und die Reaktionsziele für NTT Ltd. fest. Die Beschreibung des Support Service ist im Zusammenhang mit anderen weiter unten festgelegten Dokumenten zu lesen.

### 1.2 Dokumentenstruktur Supportvertrag

In diesem Abschnitt ist beschrieben, wie die Vertragsdokumentation strukturiert ist.



### 1.3 Begriffsbestimmungen

Die folgenden Begriffe werden in dieser Beschreibung der Support Services verwendet:

Begriff	Begriffsbestimmung
Anbieter	Ein Hersteller oder Anbieter eines Produkts oder einer Dienstleistung
Fehlerbehebung über Fernzugriff	Eine bestimmte Form der Fehlerbehebung, die Fernzugriff und das Auslesen von Protokollen und Diagnosedaten beinhaltet, um die Behebung eines Problems zu unterstützen, das im Rahmen einer Supportanfrage gemeldet wurde
Geschäftszeiten	Premium bedeutet: Sieben Tage die Woche, 24 Stunden pro Tag einschliesslich Feiertage. Standard bedeutet: 09:00 bis 17:00 Uhr Montag bis Freitag, außer an den gesetzlichen örtlichen Feiertagen (verfügbar in folgenden Zeitzonen: Mitteleuropäische Zeit MEZ, Westeuropäische Zeit WEZ oder Eastern Standard Time EST, unter Berücksichtigung der saisonalen Abweichungen, z. B. mitteleuropäische Sommerzeit, MESZ). Wenn bei Vertragsschluss nichts anderweitiges mit NTT Ltd. Support vereinbart worden ist, richten die Geschäftszeiten sich nach der Ortszeit des Landes, in dem sich die NTT Ltd. Niederlassung befindet, über die der Vertrag über Support Services geschlossen wurde.
ISP	Internet Service Provider
Kunde	Fabricant, éditeur ou distributeur d'un produit ou d'un service.
NTT Ltd.	Die NTT Ltd. (vormals NTT Com Security Limited) oder ein verbundenes Unternehmen.
Produkt	Die Soft- und Hardwareprodukte, die im Supportzertifikat beschrieben sind

Produktlizenz	Die Endbenutzerlizenzvereinbarung, die vom Eigentümer der geistigen Eigentumsrechte eines Produkts zur Verfügung gestellt wird.
Produktstandort	Jeder physische Standort, an dem ein Produkt installiert ist, um den Support Service bereitzustellen
RMA	Genehmigung für Materialrücksendung (RMA)
SecureCall	Der Telefonsupportdienst von NTT Ltd.
SecureHands	Eine proaktive technische Fernunterstützungsoption für den SecureCall-Service
Servicelevel	Premium: 24 Stunden pro Tag, 7 Tage der Woche einschliesslich Feiertage
Supportanfrage	Ein Vorfall oder eine Frage, die mit dem NTT Ltd. Ticketsystem nachverfolgt wird

## 2 Services

### 2.1 Servicelevel

SecureCall wird nur mit Servicelevel Premium geliefert, d.h. 24 Stunden pro Tag, 7 Tage der Woche.

*Bitte beachten: Die Eskalation zum Anbieter einschliesslich RMA kann nur im Zusammenhang mit dem verbundenen Level 3 Supportvertrag stattfinden.*

### 2.2 Umfang des Support Service

Der Support Service ist eine umfassende Dienstleistung, die sich am Lebenszyklus der von den Kunden genutzten Sicherheitstechnologien orientiert. Sie besteht aus einer Reihe von Basiselementen (Incident Management und Knowledge Management) und einer Reihe von optionalen Elementen, die hinzugekauft werden können. Weitere Einzelheiten dazu finden Sie unter den Punkten 3.9, 3.10, 3.11 und 3.12.

Wenn nichts anderweitiges vereinbart oder ausdrücklich im Rahmen eines optionalen Elements bestimmt ist, beachten Sie bitte, dass die Support Services Folgendes NICHT enthalten:

- Bereitstellung oder Unterstützung bei der Installation der Software, Hardware, von Upgrades, Service Packs, Funktionspaketen und Hotfixes
- Konfiguration oder Neuaufbau von Systemen
- Backup und Wiederherstellung von Systemen
- Telefonische Beratung – der Kunde kann die Option SecureHands nutzen (siehe Punkt 3.11)
- Telefonische Schulung – der Kunde kann die Option SecureHands nutzen (siehe Punkt 3.11)
- Support für Produktversionen, die außerhalb des Herstellersupports liegen
- Das SOC stellt Support Services für Soft- und Hardwareversionen der Produkte zur Verfügung, jedoch unter der Voraussetzung, dass diese weiterhin von ihrem Hersteller unterstützt werden. Wenn ein Produkt nicht mehr vom Hersteller unterstützt wird, empfiehlt das SOC als ersten Schritt bei der Lösung eines Supportproblems ein Upgrade auf eine vom Hersteller unterstützte Version. Wenn der Kunde kein Upgrade durchführen kann, kann der Kunde die Option SecureHands nutzen (siehe Punkt 3.11) und sich vom SOC Rat

über die vom Hersteller nicht unterstützte Technologie einholen. Für Produktversionen, die nicht vom Hersteller unterstützt werden, wird der Support im wirtschaftlich vertretbaren Rahmen geleistet.

- Supportanfragen mit Priorität P1 oder P2, bei denen ein technisches Problem in Bezug auf Geräte oder Konfigurationen besteht, die NICHT erfolgreich in einer Produktionsumgebung eingesetzt sind. Supportanfragen mit Priorität P3 oder P4 für solche Geräte sind im Umfang des Support Service enthalten.
- Die Behebung von Vorfällen aufgrund mangelhafter Fähigkeiten des Kunden in Bezug auf das Produkt, technisches Verständnis oder Planung
- Missbrauch des Produkts, Nutzung des Produkts außerhalb der Empfehlungen des Herstellers und/oder nicht den entsprechenden Leitlinien des Herstellers über Produkteinschränkungen und unterstützte Konfigurationen folgend
- Alle Beauftragungen von Support Services durch den Kunden bei NTT Ltd. unterliegen jederzeit der Vereinbarung über Support Services und der Beschreibung der Support Services in der jeweils geltenden Fassung. Die Dauer des beauftragten Supports ist im entsprechenden Supportzertifikat beschrieben.

### 3 Kenndaten der Support Services

#### 3.1 Ein Ansprechpartner (Single Point of Contact)

Der Kunde kann Supportanfragen beim SOC melden, die sich auf Vorfälle bei Produkten beziehen, für die aktuell eine gültige Berechtigung auf Support Services besteht.

#### 3.2 Sprachunterstützung

Es werden alle wirtschaftlich vertretbaren Anstrengungen unternommen, die Dienstleistungen während der Geschäftszeiten – Standard – in Englisch, Deutsch und Französisch zur Verfügung zu stellen. Außerhalb der Geschäftszeiten – Standard – müssen Supportanfragen in englischer Sprache gestellt werden und es kann sein, dass der Support Service auch nur in Englisch bereitgestellt wird.

#### 3.3 Technischer Support

Das SOC bietet eine technische Problemanalyse, Fehlersuche und Diagnose für die unterstützten Produkte an.

Das SOC versucht zunächst, den vermuteten Vorfall als tatsächliches Problem zu bestätigen und bittet den Kunden dazu eventuell, zusätzliche Informationen zur Verfügung zu stellen und Checks und Tests durchzuführen, um die vermutete Ursache des Problems einzugrenzen.

Der Kunde muss alle vom SOC geforderten Tests, Checks und Aktionen durchführen, um eine Abhilfe oder Übergangslösung zu finden. Dort, wo Checks durch den Kunden kein eindeutiges Ergebnis liefern oder mit dem Risiko behaftet sind, den normalen Betrieb des Systems zu beeinträchtigen, kann das SOC versuchen, das vermutete Problem intern nachzubilden und zu prüfen.

Wenn das Problem als solches bestätigt wurde, sucht das SOC weiter nach der Fehlerursache und fordert den Kunden eventuell auf, weitere Tests durchzuführen.

Wenn innerhalb eines mit dem Kunden vereinbarten angemessenen Zeitraums keine lokale Lösung oder Übergangslösung für das Problem gefunden wird, muss das SOC das Problem dem Anbieter melden, um weitere Untersuchungen zu veranlassen. Dieser Prozess der Fehlersuche und Behebung kann die Übermittlung von Kundeninformationen und Dateien an den Anbieter beinhalten.

Bitte beachten: Die Eskalation zum Anbieter einschliesslich RMA kann nur im Zusammenhang mit dem verbundenen Level 3 Supportvertrag stattfinden.

Solange eine Supportanfrage bearbeitet wird, sind regelmäßige Kommunikationsupdates zwischen dem SOC und dem Kunden zu vereinbaren.

#### 3.4 Hardware Support – einschließlich RMA

Wenn der Kunde Hardware-Support erworben hat, sorgt das SOC für die Hardware-Fehlerdiagnose und die Weiterleitung an den Hardware-Support des Anbieters gemäß dem gebuchten Hardware-Support.

Reaktionszeiten und Servicelevel für Hardwareersatz sind vom Level des gebuchten Hardware-Supports abhängig. (Eine RMA ist mit dem Anbieter abzustimmen und kann eine tägliche Schlusszeit beinhalten, innerhalb der der RMA zu verarbeiten ist.) Die RMA-Reaktionszeit beginnt, sobald ein Hardware-Problem vom Anbieter autorisiert worden ist.

Der Kunde sollte in seinem Supportzertifikat nachlesen oder im Online-Portal von SecureCall (Punkt 3.7) und/oder sich an seinen Kundenberater wenden, um sich die Einzelheiten des von ihm erworbenen Hardware-Supports bestätigen zu lassen.

Bitte beachten: Die Eskalation zum Anbieter einschliesslich RMA kann nur im Zusammenhang mit dem verbundenen Level 3 Supportvertrag stattfinden.

#### 3.5 Management von Supportanfragen

In diesem Abschnitt wird das Management von Supportanfragen für SecureHands und die Bewertung der Technologiebasis nicht behandelt; dies wird eigens unter Punkt 3.11 beschrieben.

##### 3.5.1 Bearbeitung von Supportanfragen

Supportanfragen werden beim SOC eingereicht. Die Supportanfrage wird im NTT Ltd. Ticket-Managementsystem eingereicht und der Kunde erhält automatisch eine Referenznummer (Service Request ID), unter der die Anfrage verarbeitet wird. Der Kunde sollte die Service Request-ID in allen Mitteilungen in Bezug auf die bestimmte Anfrage angeben.

### 3.5.2 Einreichen/Generieren von Supportanfragen

Supportanfragen können wie folgt eingereicht werden:

Meldung des Vorfalls per	Einschränkungen	Zeitfenster für die Meldung
Telefon <sup>1</sup>	Alle Prioritäten	24h/7 <sup>3</sup>
E-mail <sup>2</sup>	Nur Prioritäten 2, 3 und 4	24h/7 <sup>3</sup>
Web-Portal	Nur Prioritäten 2, 3 und 4	24h/7 <sup>3</sup>

<sup>1</sup> Alle dringenden Probleme, z. B. Supportanfragen der Priorität 1, sind telefonisch zu melden. MARTYN'S NOTE: „Gemäß Servicelevel“ is now redundant but I cannot remove it from the table

<sup>2</sup> Supportanfragen, die per E-Mail gemeldet werden, erhalten standardmäßig die Priorität 3 und werden automatisch per E-Mail bestätigt. Die Standardpriorität kann geändert werden. Wenden Sie sich dazu telefonisch an das SOC, nachdem die Supportanfrage generiert wurde.

<sup>3</sup> Per E-Mail und über das Portal eingereichte Supportanfragen werden auf der Basis 24/7 überwacht und bearbeitet.

### 3.5.3 Erste Reaktion Servicelevel

Wenn eine Supportanfrage eingereicht wird, ist diesem eine Priorität zuzuweisen, und zwar gemäß der unten stehenden Tabelle. This sentence is redundant IMO. In der Tabelle unten sind auch die Zielzeiten für die erste Reaktion festgelegt. Erste Reaktion bedeutet, dass ein Mitarbeiter des SOC bestätigt, dass eine Supportanfrage generiert wurde, und nicht, dass das Problem gelöst ist.

Priorität der Supportanfrage	Auswirkung des Vorfalls	Zielzeiten erste Reaktion
1	Produktionssystem funktionsunfähig oder nicht nutzbar	30 Minuten
2	Produktionssystem ist teilweisenutzbar oder es steht eine	2 Stunden
3	Geringer Einfluss auf Betrieb	24 Stunden
4	Keine Auswirkung auf Betriebszustand des Produkts	2 Tage

### 3.5.4 Fehlerbehebung über Fernzugriff

Die Fehlerbehebung über Fernzugriff ist eine bestimmte Form der Fehlerbehebung und Erhebung von Diagnosedaten, die auf Basis einer Technologie wie z. B. Cisco WebEx (derzeit im SOC im Einsatz) erfolgt. Wenn der Kunde seine eigene Fernzugriffstechnologie nutzen möchte, muss er das SOC darüber informieren. Die Nutzung der eigenen Technologie für Fehlerbehebung im Fernzugriff erfolgt auf eigenes Risiko des Kunden.

Die Fehlerbehebung im Fernzugriff erfolgt nur im eigenen Ermessen des SOC. Die Zugriffsebene (nur Ansicht/Ansicht und Steuerung) ist mit dem Kunden zu vereinbaren.

Wenn der Kunde Unterstützung bei anderen Handlungen wie z. B. der Installation von Patches oder Konfigurationsänderungen benötigt, sollte der Kunde die Option SecureHands nutzen (siehe Punkt 3.11).

Der Kunde sollte sich dessen bewusst sein, dass die Fehlerbehebung im Fernzugriff Auswirkungen auf die Leistung des Kundensystems haben oder sich anderweitig negativ auswirken kann, z. B. Geräteunzugänglichkeit, Geräteausfall oder Netzwerkprobleme. Der Kunde bestätigt, dass NTT Ltd. dem Kunden gegenüber nicht für etwaige Ausfälle von Diensten oder Schäden des Kunden oder eines Dritten haftet, die diesen diesbezüglich entstehen, und zwar weder direkte noch Folgeschäden. Der Kunde stellt NTT Ltd. hiermit frei und hält es schadlos von und gegenüber allen Forderungen durch den Kunden oder Dritte, die durch das Erfassen von Diagnosedaten durch NTT Ltd. entstehen.

NTT Ltd. behält sich das Recht vor, Änderungen an der Art der Durchführung der Fehlerbehebung im Fernzugriff vorzunehmen, ohne den Kunden im Voraus darüber zu benachrichtigen. Fehlerbehebungssitzungen im Fernzugriff können von NTT Ltd. oder vom Kunden aufgezeichnet werden.

### 3.5.5 Überwachung von Supportanfragen

Der Standardüberwachungsprozess für Supportanfragen sieht vor, dass das SOC und der Kunde Informationsintervalle und voraussichtliche Reaktionszeiten vereinbaren.

Die folgende Tabelle beschreibt den Prozess, der für die Überwachung von Supportanfragen eingehalten wird:

Service Request Priority				
	1	2	3	4
Erste Reaktion auf Supportanfragen	Reaktion von 30 Minuten	Reaktion von 2 Stunden	Reaktion von 24 Stunden	Reaktion von 2 Tage
Überwachung der Supportanfrage	Tägliche Prüfung von Supportanfragen durch das SOC			
	Automatische E-Mail Warnung wird an das SOC gesandt, wenn Supportanfragen nicht aktualisiert werden.			
	SOC Teamleiter regeln regelmäßige Fortschrittsprüfungen aller offenen Supportanfragen			

### 3.5.6 Eskalation von Supportanfragen

- Der Kunde ruft direkt beim NTT Ltd. SOC an und bittet um Eskalation der Supportanfrage.
- Das SOC eskaliert dann das Problem an das Team „Duty Management“ weiter.
- Nach Prüfung der Supportanfrage wird der Eskalationskontakt dann eine für den jeweiligen Vorfall angebrachte Maßnahme umsetzen.
- Der Ansprechpartner beim Kunden, der die Eskalation angefordert hatte, wird über die Maßnahme informiert und es werden regelmäßige Informationsintervalle vereinbart.
- Gegebenenfalls wird an diesem Punkt der Kundenberater des Kunden (und gegebenenfalls auch der Service-Manager) benachrichtigt.
- Eine weitere Eskalation auf Direktorebene kann veranlasst werden, wenn die Eskalation länger als 3 Tage andauert (nach 24 Stunden bei Priorität 1 (Probleme mit Systemausfall)).
- Alle Eskalationen werden zentral innerhalb des SOC nachverfolgt.
- Eskalationen werden zwecks kontinuierlicher Verbesserung des Serviceprozesses analysiert.

### 3.5.7 Abschluss von Supportanfragen – Ursachenanalyse

Um etwaige Zweifel auszuräumen sei darauf hingewiesen, dass die Fehlerbehebung im Rahmen einer Supportanfrage keine Ursachenanalyseberichte beinhaltet.

Kunden können die Ursachenanalyse eines aufgetretenen Problems anfordern und diese Anforderungen können im Rahmen der Option SecureHands bearbeitet werden. (Siehe Punkt 3.11)

### 3.6 Best Practices für Update und Upgrade

Dem Kunden wird stark angeraten, Systemänderungen und Upgrades wie folgt anzugehen, um die Support Services bestmöglich zu nutzen und Ausfallzeiten zu reduzieren.

- Änderung/Upgrade im Voraus planen.
  - Wenden Sie sich an den SOC und erläutern Sie, was Sie planen. Das SOC kann Ihnen möglicherweise Ratschläge dahingehend geben, welche Auswirkungen die Änderungen haben könnten und welche Probleme möglicherweise auftreten können.
  - Lesen Sie die Mitteilungen des Support Update Service (siehe Punkt 3.8) zu den relevanten Themen.
- Erstellen Sie vor der Änderung/dem Upgrade einen Backup, um einen Wiederherstellungspunkt zu haben.

- Testen Sie die Änderung/das Upgrade vor der Implementierung auf einem Produktionssystem auf einem nicht geschäftskritischen System.
  - Um etwaige Mängel an Ressourcen, Erfahrung, Wissen oder Qualifikationen auszugleichen, stehen Vorort-Dienste über die NTT Ltd. Professional Services (siehe Punkt 3.9) zur Verfügung, falls der Kunde wünscht, dass NTT Ltd. die Änderungen oder Upgrades durchführt. Als Alternative kann die Option SecureHands (siehe Punkt 3.11) genutzt werden, die Fernunterstützung für die Durchführung von Änderungen, Updates oder Upgrades bietet). Diese Dienste müssen im Voraus beauftragt werden.

### 3.7 Zugang zum Online-Portal von SecureCall

Das Online-Portal von SecureCall bietet dem Kunden folgende Möglichkeiten:

- Öffnen, Anzeigen und Aktualisieren von Supportanfragen
- Abrufen von Einzelheiten und Status von Supportanfragen
- Anzeigen von Berichten
- Anzeigen der Produkte mit Support, einschließlich deren Wartungs-/Support-Berechtigungen (Ressourcenverwaltung)
- Hoch- und Herunterladen von Diagnosedateien, die im Rahmen der technischen Fehlerbehebung erforderlich sind
- Anzeigen von Dokumentation im Zusammenhang mit dem Support Service
- Das Online-Portal von SecureCall ist nur in englischer Sprache verfügbar. Es ist über den folgenden Link erreichbar: <https://support.nttsecurity.com>
- Der Zugang zum Online-Portal von SecureCall kann über eine Supportanfrage beim SOC angefordert werden. Das SOC kann dem Kunden auch das neuste Portalhandbuch zur Verfügung stellen, um sich im Portal leichter zurechtzufinden.

### 3.8 Support Update Service (SUS)

Der Support Update Service ist ein wertvoller E-Mail-Service, der Kunden zur Verfügung steht, die sich rechtzeitig über Ratschläge zu Patches, Software-Updates sowie wichtige technische Bekanntmachungen für Produkte informieren lassen möchten, die über den Support Service unterstützt werden.

NTT Ltd. haftet nicht für die Richtigkeit und die rechtzeitige Verbreitung der Informationen, die von Hardware- und Softwareherstellern zur Verfügung gestellt werden. Der Support Update Service steht nur in englischer Sprache zur Verfügung.

Der Kunde muss sich für den SUS-Service anmelden. Zwecks An- oder Abmeldung zu oder von diesem Dienst wenden Sie sich bitte an das SOC.

### 3.9 Vor-Ort-Unterstützung (kostenpflichtige Option)

Die Vor-Ort-Unterstützung ist nicht im SecureCall-Service enthalten. Wenn diese beauftragt wird, wird sie lokal bereitgestellt und gemäß den lokalen Richtlinien durchgeführt, und zwar unter Einhaltung der für die Professional Services gültigen lokalen Bedingungen.

### 3.10 Technischer Account-Manager (kostenpflichtige Option)

Durch die Pflege langfristiger Kundenbeziehungen erhält der Technische Account-Manager (TAM) wertvolle Informationen über die Sicherheitssysteme, die Organisation und das gesamte Geschäft des Kunden und in die Ziele und Problembereiche der Informationssicherheit.

Die TAM-Funktion wird nur während der „Geschäftszeiten – Standard“ zur Verfügung gestellt. Dem Kunden wird zudem ein namentlich benannter SOC-Sicherheitsanalytiker zugewiesen, der über umfangreiche Erfahrung im Bereich Sicherheit und über tief greifende Kenntnisse in der Fehlerbehebung verfügt, die für das Netzwerkprofil und die Operationsanforderungen des Kunden maßgeblich sind.

- Technischer Ansprechpartner (Single Point of Contact) – der TAM fungiert als dezidiertes Eskalationskontakt für Probleme im Zusammenhang mit dem Support Service, einschließlich der Eskalation von Supportanfragen, und bietet zusätzliche technische Expertise und koordiniert Angelegenheiten in Bezug auf den Support Service.
- Beschleunigte Lösung technischer Probleme – der TAM wird über alle Supportanfragen und sonstige Probleme benachrichtigt, die vom Kunden gemeldet werden, insbesondere solche mit höherem Schweregrad, wo der TAM als zusätzliche Ressource zur Lösung des Problems dient. In enger Zusammenarbeit mit dem Kunden koordiniert der TAM das Vorfalldmanagement des Kunden und die Problemmanagement-Aktivitäten, indem er die entsprechenden Ressourcen einschaltet, um die Probleme mit minimaler Störung des Geschäftsbetriebs des Kunden zu lösen.
- Beachtung des Produktlebenszyklus – der TAM stellt sicher, dass die unterstützten Technologien für den Security Update Service (SUS) registriert werden, so dass der Kunde den Produktlebenszyklus kennt, und dieses Element wird im Rahmen der regulären Meetings besprochen.
- Flexibles aktives Engagement – der TAM organisiert und nimmt an Kundenmeetings teil, und zwar in der Häufigkeit wie mit dem Kunden vereinbart. Insgesamt werden vier Kundenmeetings (eines pro Quartal) pro Jahr empfohlen. Weitere oder häufigere Meetings sind möglich und können vom Kunden gegen zusätzliches Entgelt angefordert werden. Kundenmeetings können am Standort des Kunden (innerhalb Europas) durchgeführt werden oder im SOC (derzeit mit Sitz in Großbritannien), wo ein direkter persönlicher Kontakt mit dem Support-Team möglich ist, oder telefonisch

bzw. als Fernsitzung. Die am besten geeignete Form des Kundenmeetings ist mit dem Kunden zu vereinbaren. Bei den Meetings werden die Verläufe der Supportanfrage und die eingerichteten Maßnahmenpläne besprochen, sowie etwaige künftige Änderungen des Geschäfts oder der Infrastruktur des Kunden.

### 3.11 SecureHands – Technische Unterstützung per Fernzugriff (kostenpflichtige Option)

Mit der Option SecureHands stehen die hochqualifizierten Mitarbeiter des SecureCall-Teams Kunden auch bei Aufgaben zur Seite, die über den grundsätzlichen Rahmen des Support Service (gemäß der Beschreibung unter den Punkten 3.1 bis 3.8) hinausgehen. SecureHands ergänzt somit die unternehmensinternen technischen Kompetenzen und Kapazitäten der Kunden, wenn dies erforderlich ist und SOC-Kapazitäten verfügbar sind. Die von SecureHands abgedeckten Technologien sind eine Untergruppe der von SecureCall abgedeckten Technologien. Bezüglich Informationen zu in Frage kommenden Technologien wenden Sie sich bitte an Ihren Kundenbetreuer.

Die folgende Tabelle zeigt einige Beispiele für typische Nutzungsarten von SecureHands:

SecureHands-Typ	Typische Nutzung
Umsetzung von Änderungen	Änderungsimplementierung, Funktionsaktivierung
Support per Fernzugriff auf Anfrage	Beratung während einer Neuinstallation oder eines Systemneuaufbaus/ Unterstützung über den Umfang von SecureCall hinaus/ Unterstützung Geräte ohne Herstellersupport/ Einführung für Produkt/ Technologie
Bearbeitung von speziellen Anfragen	Je nach Kundenanforderung, einschließlich Fehlerbehebung im Fernzugriff (siehe 3.5.4.1), Ursachenanalyse (siehe 3.5.7)
Bewertung der Technologiebasis (Technical Baseline Assessment)	Funktionsprüfung eines oder mehrerer Sicherheitsgeräte
Schulung	Wir bieten Fern-bzw. Onlineschulungen zu einer Reihe von Themen an, darunter anbieterspezifisches Troubleshooting, Konfiguration, Patching/Upgrades und Administration. Auch allgemeinere Themen wie etwa http/https, Best Practices für DNS
Aktualisierungen	Patch, Hotfix und kleinere Software upgrades

SecureHands wird in Zusammenarbeit zwischen dem SOC und dem Kunden erbracht, als Kombination aus Telefonunterstützung und technologischer Fernwartung – siehe Fehlerbehebung im Fernzugriff.

Die rechtlichen Bedingungen bezüglich der Erbringung der SecureHands-Leistungen sind die, die der Leistungsbeschreibung beigelegt sind. Die SecureHands-Leistungsbeschreibung ist die Beschreibung der Maßnahmen (technischer und anderer), die im Rahmen von einer oder mehreren zusammengehörigen SecureHands-Sitzungen durchgeführt werden. Die Leistungsbeschreibung ist vom SOC auf Grundlage der vom Kunden zur Verfügung gestellten Anforderungen zusammenzustellen, von beiden Parteien zu vereinbaren und vom Kunden zu genehmigen, bevor die entsprechende(n) SecureHands-Sitzung(en) eingeplant wird/werden. Wenn die Leistungsbeschreibung vereinbart ist und unter der Voraussetzung, dass der Kunde über genügend Einheiten verfügt, um die in der vereinbarten Leistungsbeschreibung festgelegten Maßnahmen abzudecken, werden die SecureHands-Sitzungen gemeinsam mit dem Kunden geplant. Die Sitzungsdauer ist über die Vereinbarung der Leistungsbeschreibung festzulegen. Bitte beachten Sie, dass eine Leistungsbeschreibung mehrere Sitzungen umfassen kann. Wenn in der Leistungsbeschreibung nichts anderes vereinbart ist, beinhaltet eine SecureHands-Sitzung jegliche Vorbereitungs- oder Dokumentationszeit, die für die Leistungsbeschreibung verbraucht wurde. Eine SecureHands-Sitzung folgt der vereinbarten Leistungsbeschreibung und jegliche Abweichung kann eine Neuformulierung der Leistungsbeschreibung notwendig machen. Das SOC kann die Anforderung von SecureHands-Leistungen ablehnen, wenn im alleinigen Ermessen des SOC die technischen Kapazitäten für die Erfüllung der Anforderungen, des Zeitrahmens oder der geforderten Planung nicht zur Verfügung stehen. Der Kunde kann an das Team der NTT Ltd. Professional Services verwiesen werden, wenn die angeforderten Maßnahmen von SecureHands nicht abgedeckt werden können.

NTT Ltd. nimmt möglicherweise Kontakt mit Kunden auf, die über ungenutzte SecureHands-Einheiten verfügen, die noch nicht von einer vereinbarten Leistungsbeschreibung abgedeckt sind, um die Nutzung dieser SecureHands-Einheiten zu besprechen.

### 3.11.1 SecureHands-Leistungszeiten und Sprachen

Die SecureHands-Leistungszeiten (für Management der Supportanfragen und Leistungserbringung) sind die „Geschäftszeiten – Standard“, wenn über die Leistungsbeschreibung mit dem SOC nichts anderes vereinbart ist.

Jede Kommunikation mit dem SOC und alle schriftlichen Unterlagen (einschließlich der Leistungsbeschreibung) müssen in Englisch sein. Dort, wo entsprechende Ressourcen verfügbar sind, kann SecureHands auch in Französisch oder Deutsch erbracht werden, wenn der Kunde dies wünscht.

### 3.11.2 Beschaffung und SecureHands-Einheitenmanagement

Die Option SecureHands ist als kostenpflichtige Option des Support Service zu erwerben. SecureCall ist eine Voraussetzung für den Erwerb von SecureHands, wenn nichts anderes vereinbart ist. Einheiten sind im Voraus, vor Durchführung der Sitzung(en), zahlbar.

SecureHands-Einheiten sind 12 Monate lang gültig und laufen am Ende ihrer Gültigkeitsdauer ab.

- Wenn eine Leistungsbeschreibung vereinbart wird, dann werden die Einheiten, die für die Verwendung für die Leistungsbeschreibung eingeplant sind, aus den aktuell verfügbaren Einheiten reserviert.
- Nach Erbringung und Annahme jeder SecureHands-Sitzung:
  - Wenn eine feste Anzahl von Einheiten zwischen den Parteien der Leistungsbeschreibung vereinbart worden ist, dann wird der Saldo der Einheiten mit der vereinbarten festen Anzahl von Einheiten für jede SecureHands-Sitzung belastet.
  - In allen anderen Fällen wird der Saldo der Einheiten mit den tatsächlich für jede

SecureHands-Sitzung verwendeten Einheiten belastet.

- SecureHands-Sitzungen werden mit der für die Sitzung aufgewendeten Zeit belastet, und zwar in Stunden, aufgerundet auf die nächste Stunde. Wenn sie während den Leistungszeiten erbracht werden, die unter 3.11.2 festgelegt sind, dann entspricht eine Stunde einer SecureHands-Einheit.
- Für SecureHands-Sitzungen, die außerhalb der „Geschäftszeiten – Standard“ erbracht werden, ist die Anzahl der pro Stunde belasteten Einheiten eine andere. Dies wird in der Leistungsbeschreibung festgelegt.
- Der Kunde muss die verfügbaren Einheiten möglicherweise aufstocken, wenn die Anzahl der Einheiten nicht ausreicht, um die in der Leistungsbeschreibung definierten Arbeiten durchzuführen. NTT Ltd. muss dem Kunden unverzüglich ein Angebot über die Differenz an SecureHands-Einheiten machen und der Kunde vereinbart, innerhalb von 30 Tagen nach Eingang eines solchen Angebots einen Auftrag zu erteilen, um die fehlenden SecureHands-Einheiten auszugleichen.

### 3.11.3 Stornierung einer SecureHands-Sitzung

Wenn eine geplante Sitzung vom Kunden innerhalb von zwei Arbeitstagen vor dem geplanten Beginn storniert wird oder wenn der Kunde zu einer geplanten Sitzung nicht erscheint, dann verfällt die Anzahl der SecureHands-Einheiten im Zusammenhang mit dieser geplanten Sitzung und der Saldo der SecureHands-Einheiten wird sofort mit derselben Anzahl belastet.

Eine geplante SecureHands-Sitzung, die von einer der Parteien aus Gründen storniert wird, die außerhalb deren Kontrolle liegen, wird neu eingeplant, und zwar zu einem Termin, der für beide Parteien geeignet ist.

### 3.11.4 Management von SecureHands Supportanfragen

Der Kunde reicht die SecureHands-Supportanfrage telefonisch oder per E-Mail beim SOC ein (gemäß demselben Verfahren wie unter Punkt 3.5.2 beschrieben). Dem Kunden wird stark empfohlen, diese Supportanfrage als „SecureHands“ bzw. als „Bewertung der Technologiebasis (TBA) zu kennzeichnen.

Das SOC kann vom Kundenbetreuer fordern, sich selbst positiv zu identifizieren.

Der Kunde darf eine unbegrenzte Anzahl von SecureHands-Supportanfragen generieren; dies gilt vorbehaltlich der Klassifizierung als „fairer Gebrauch“ im alleinigen Ermessen von NTT Ltd.

### 3.11.5 SecureHands Servicelevel-Ziele

Es gelten die folgenden Servicelevel-Ziele:

Beschreibung	Reaktionszielzeiten
Erste Reaktion auf eine SecureHands-Supportanfrage	8 Arbeitsstunden
Reaktionszielzeit Leistungsbeschreibung	2 Arbeitstage nach Anfrage
Planung von SecureHands Sitzung (vorausgesetzt, dass bereits eine Leistungsbeschreibung vereinbart ist)	3 Arbeitstage nach Anfrage über eine SecureHands Sitzung

### 3.11.6 Abschluss und Annahme von SecureHands-Sitzungen

Nachdem eine SecureHands-Sitzung abgeschlossen ist, sendet das SOC einen Abschlussbericht über die SecureHands-Sitzung an den Kunden, welcher:

- die Zeit und Summe der in der SecureHands-Sitzung verbrauchten SecureHands-Einheiten angibt.
- den Kunden über den aktuellen Saldo der SecureHands-Einheiten informiert.
- um Kundenfeedback über die SecureHands-Sitzung bittet.

Die Annahme der SecureHands-Sitzung muss gemäß den Annahmekriterien erfolgen, die in der Leistungsbeschreibung festgelegt sind. Wenn in der Leistungsbeschreibung nichts anderes festgelegt ist und wenn der Kunde keine Reklamation bezüglich einer SecureHands-Sitzung macht, gilt eine SecureHands-Sitzung zwei Arbeitstage nach Versand des SecureHands-Sitzungsabschlussberichts als vom Kunden angenommen.

### 3.11.7 SecureHands-Servicegutschriften

Sollte der Kunde eine Reklamation in Bezug auf die Annahme einer SecureHands-Sitzung einreichen, und zwar innerhalb von zwei Arbeitstagen nach Absendung des SecureHands-Sitzungsabschlussberichts, dann untersucht das SOC-Management die Reklamation gemeinsam mit dem Kunden. Innerhalb von 5 Arbeitstagen ab Eingang der Reklamation des Kunden kann NTT Ltd. in seinem alleinigen Ermessen die Belastung der SecureHands-Einheiten des Kunden stornieren, und zwar bezüglich aller oder eines Teils der SecureHands-Einheiten, die für die reklamierte SecureHands-Sitzung genutzt wurden.

## 3.12 Bewertung der Technologiebasis (kostenpflichtige Option)

### 3.12.1 Übersicht der Service-Optionen

Im Rahmen der Bewertung der Technologiebasis werden die kritischen Sicherheitseinrichtungen eines Kunden mithilfe der Best Practices der Branche auf ihre Zwecktauglichkeit hin überprüft.

Die Bewertung der Technologiebasis erfolgt mithilfe des Mechanismus der technischen Unterstützung per Fernzugriff (siehe Punkt 3.11), welcher eine vereinbarte Leistungsbeschreibung und identifizierte Ressourcen beinhaltet. Die rechtlichen Bedingungen bezüglich der Erbringung der technischen Unterstützung per Fernzugriff sind die, die der Leistungsbeschreibung beigelegt sind. Wie in der Leistungsbeschreibung definiert und vereinbart kann für jede Bewertung ein Bericht zur Verfügung gestellt werden, der die Befunde und gegebenenfalls Empfehlungen für Verbesserungen enthält.

Die Beschreibung der technischen Unterstützung per Fernzugriff unten beschreibt den allgemeinen Umfang und dient als allgemeine Leitlinie. Im Falle einer Unstimmigkeit zwischen der Beschreibung unten und der Leistungsbeschreibung gilt die Leistungsbeschreibung vorrangig.

Die technische Unterstützung per Fernzugriff für eine Sicherheitseinrichtung dient der Erkennung von Unzulänglichkeiten und Schwachstellen an einer Sicherheitseinrichtung, bevor diese kritisch werden. Das SOC identifiziert, klassifiziert und priorisiert Probleme gemäß deren Kritizität, Auswirkung und ihrem allgemeinen Schweregrad und empfiehlt Abhilfemaßnahmen für die Zukunft. Diese Abhilfemaßnahmen beinhalten etwaige empfohlene Änderungen und eine Analyse der Auswirkungen jeder einzelnen Empfehlung. Alle diese Informationen werden in einem schriftlichen Bericht an den Kunden dargestellt. Danach können weitere Arbeiten über die Option SecureHands oder Vor-Ort-Unterstützung arrangiert werden.

Die Bewertungen werden für jedes Produkt individuell durchgeführt und können die Prüfung der Hardware, Software, des Netzwerks, der Hochverfügbarkeit, der Systemdienstleistungen und Verwaltung beinhalten.

### 3.13 Schwachstellenanalyse (kostenpflichtige Option)

#### 3.13.1 Schwachstellenanalyse

Die Schwachstellenanalyse liefert dem Kunden einen Bericht über die Schwachstellen, die potenzielle Hacker finden und ausnutzen können.

Die Analyse umfasst einen externen, nicht authentifizierten Scan der vom Kunden definierten und in der Leistungsbeschreibung genannten IP-Adressen im Umfeld des Kunden. Dazu werden maximal 25 externe IP-Adressen gescannt. Auf Anfrage und in Abstimmung mit dem SOC kann jedoch auch eine größere Anzahl gescannt werden. Pro Auftrag sind maximal zwei Scans der gleichen Gruppe von IP-Adressen eingeschlossen.

1. 1.Scan: In diesem ersten Schritt werden die von einem Kunden bereitgestellten IP-Adressen gescannt. Dieser Scan bildet die Grundlage für den Bericht und alle daraus folgenden Empfehlungen.
2. 2.Scan: Der zweite Scan wird durchgeführt, nachdem der Kunde selbst oder mithilfe von SecureHands-Einheiten (siehe 3.11) alle erforderlichen Maßnahmen zur Behebung der im ersten Scan gefundenen Schwachstellen abgeschlossen hat. Mit diesem zweiten Scan wird nur geprüft, ob diese Schwachstellen beseitigt wurden. Es werden weder weitere Ressourcen geprüft noch neue Schwachstellen identifiziert. Der zweite Scan muss innerhalb von 30 Tagen nach der Prüfung des Berichts angefordert und innerhalb von 45 Tagen nach der Prüfung des Berichts durchgeführt werden. Das Anfordern des zweiten Scans liegt in der Verantwortung des Kunden.

Nachdem der Scan durchgeführt wurde,

- wird den vom Kunden festgelegten Ansprechpartnern ein Bericht zugestellt. (Hinweis: Ein beim Kunden installiertes IPS beeinträchtigt möglicherweise die Scanleistung und die Berichtsergebnisse.)
- wird ein SOC-Sicherheitsanalyst den Bericht prüfen und den vom Kunden festgelegten Ansprechpartnern weitere Empfehlungen zum Schutz gegen Schwachstellen geben. Die Prüfung wird während der Standardgeschäftszeiten durchgeführt. Sowohl der Schwachstellenbericht als auch die Prüfung werden in englischer Sprache geliefert.

Die Scans können in Abstimmung mit dem verfügbaren SOC-Personal terminlich nach Wunsch des Kunden durchgeführt werden. Wenn eine Terminverschiebung notwendig ist, muss das SOC-Team zwei Werktage vor dem geplanten Scantermin informiert werden.

Schwachstellenanalysen können jederzeit erworben und innerhalb von 12 Monaten nach Eingang des Auftrags bei NTT Ltd. eingelöst werden.

#### 3.13.2 Anforderung von Schwachstellenanalysen

Ein Schwachstellenanalyse-Ticket kann nach demselben Verfahren wie unter Punkt 3.5.2 beschrieben telefonisch oder per E-Mail beim SOC eingereicht werden. Es wird empfohlen, ein solches Ticket als „Schwachstellenanalyse“ zu kennzeichnen.

#### 3.13.3 Zielsetzung einer Schwachstellenanalyse

Für eine Schwachstellenanalyse gelten die folgenden Servicelevel:

Beschreibung	Reaktionszeiten
Erste Reaktion auf die Anforderung einer Schwachstellenanalyse	8 Arbeitsstunden
Terminierung eines Scans	Drei Werktage nach Erhalt der unterschriebenen Leistungsbeschreibung, in die die IT-Adressen des Kunden sowie Ansprechpartner angegeben sind

## 4 Sicherheitstechnik-Training (STT)

### 4.1 Kursbeschreibung

Training wird von unserer TSS-Abteilung via WebEx-Fernsitzung für Gruppen bis zu maximal 5 Teilnehmern gegeben (Training für umfangreichere Gruppengrößen kann auch von TSS angefordert werden).

Die Sitzungen werden von einem hocherfahrenen und -ausgebildeten Techniker mit geplanten Maximaldauer von 3 Stunden geleitet. Inbegriffen sind Präsentationsdias, echte Labor-Beispiele zum Üben und die Möglichkeit, Fragen zu stellen.

Weitere Angaben finden Sie in unserem Security Technology Training (STT) Katalog.

Die in der Sitzung verwendeten Materialien werden von NTT Ltd. erstellt und haben keinerlei Verbindung mit dem offiziellen Zertifizierungstraining der entsprechenden Produktherstellern.

## 5 Verantwortlichkeiten

### 5.1 Verantwortlichkeiten des Kunden

#### 5.1.1 Allgemeine Verantwortlichkeiten des Kunden

Der Kunde stellt sicher, dass die von NTT Ltd. getroffenen Maßnahmen in Verbindung mit dem Support Service im Sinne des geltenden Rechts in jedweder Gerichtsbarkeit, in der der Kunde operiert, und gemäß jedem Vertrag über die Nutzung solcher Netzwerke und Systeme als vom Kunden und allen Dritten genehmigt gelten.

Der Kunde garantiert, dass NTT Ltd. berechtigt ist, gemäß allen Informationen und Anweisungen zu handeln, die NTT Ltd. von einem Mitarbeiter des Kunden zur Verfügung gestellt wurden.

Bezüglich aller Funktionen und Optionen des Support Service muss der Kunde:

- über gültige Produktlizenzen für alle unterstützten Produkte verfügen und sicherstellen, dass diese jederzeit alle Produktlizenzbedingungen erfüllen.
- Für die Fehlersuche und das Management des Gerätes oder der Lösung, die von SecureCall Wartung gedeckt sind, muss der Kunde die entsprechenden Adminzugänge zu den admin/management gui/console haben.
- sicherstellen, dass die Verlängerung jeden Support-Service-Vertrags rechtzeitig erfolgt.

- die Verantwortung für die rechtzeitige Installation von Patches und Updates übernehmen, wo dies angemessen ist.
- regelmäßig Backups aller Daten auf den unterstützten Geräten erstellen.
- mit dem SOC bei Anfragen nach positiver Identifizierung des Kundenbetreuers zusammenarbeiten.
- Personal mit adäquater technischer Kompetenz und Ausbildung bereithalten, um NTT Ltd. bei der Fehlersuche und -behebung sowie der Problemlösung zu unterstützen. Der Kunde beschränkt den Zugang zum SOC auf dieses adäquat qualifizierte Personal und benachrichtigt das SOC über alle Einsteiger/Versetzen/Ausscheider zum Zwecke der Zugriffsverwaltung.
- die erforderlichen Informationen bereitstellen, um es dem SOC zu ermöglichen, das dem Supportvertrag unterliegende Produkt und den entsprechenden Supportvertrag eindeutig zu identifizieren, z. B. per Lizenzschlüssel, MAC-Adresse oder Seriennummer.
- mit NTT Ltd. bei der Fehlersuche und -behebung und bei der Diagnose von Vorfällen zusammenarbeiten.
- NTT Ltd. oder von NTT Ltd. bestimmten Unterauftragnehmern solchen Zugang gewähren und schriftliche Genehmigungen für die Infrastruktur und Anwendungen des Kunden erteilen, die angemessenerweise für die Erbringung der Support Services erforderlich sind, und sicherstellen, dass dieser Zugang den Informationssicherheitsrichtlinien des Kunden entspricht.
- für die Kontaktaufnahme durch das SOC oder den Anbieter zur Verfügung stehen und den Maßnahmen beiwohnen, die für den Fortschritt eines Supportanfrage notwendig sind, wenn dies von NTT Ltd. oder dem Anbieter verlangt wird, und NTT Ltd. die technischen Informationen akkurat und rechtzeitig zur Verfügung stellen, die von NTT Ltd. oder dem Anbieter angefordert werden.
- im Falle der Fehlerbehebung im Fernzugriff oder von SecureHands über die gesamte Dauer der Sitzung anwesend sein und über die gesamte Zeit der SecureHands-Sitzung physischen Zugang zum Gerät haben.
- Falls der Kunde eine oder mehrere der oben festgelegten Pflichten nicht erfüllt, haften NTT Ltd. und seine Unterauftragnehmer nicht für etwaige Fehlversuche, den Support Service zu leisten, und NTT Ltd. hat dann ein Recht auf die Kosten, die NTT Ltd. vom Unterauftragnehmer berechnet werden, um den Support Service zu leisten oder zu beheben, wobei als vereinbart gilt, dass dieser Betrag die angemessenen Kosten darstellt, die NTT Ltd. vergeblich entstanden sind.

Der Kunde trägt auch die folgende zusätzliche Verantwortung für den Support der Hardwaregeräte:

- Sicherstellen, dass NTT Ltd. über etwaige Änderungen des Produktstandortes informiert ist, indem NTT Ltd. unverzüglich aber nicht später als 30 Tage vor einem Besuch am Standort schriftlich darüber benachrichtigt wird.
- Zurücksendung fehlerhafter Hardware an den Anbieter, sobald dies vernünftigerweise praktikabel ist (gemäß den Anweisungen im RMA-Prozess) Falls der Kunde es versäumt, die fehlerhafte Hardware innerhalb des im Hardwarevertrag genannten Zeitraums zurückzusenden, behält sich NTT Ltd. das Recht vor, dem Kunden eine Gebühr zu berechnen, die der Gebühr entspricht, die NTT Ltd. vom Anbieter für die versäumte Rücksendung der Hardware belastet wird.
- Zahlung der Transport- und Zollkosten für den RMA-Prozess, der oben beschrieben ist (wenn diese nicht durch den Hardware-Support des Anbieters abgedeckt sind)

### 5.1.2 Fehlerbehebung im Fernzugriff und SecureHands

Der Kunde muss:

- im Rahmen von SecureHands mit dem SOC bei der Erstellung einer akkuraten Leistungsbeschreibung zusammenarbeiten und alle Fragen des SOC bezüglich der Erstellung der Leistungsbeschreibung beantworten.
- über einen Notfall- oder Rollbackplan verfügen, der dem SOC im Rahmen der Leistungsbeschreibung kommuniziert werden muss, falls eine Fernzugriffssitzung fehlschlägt und während einer SecureHands-Sitzung nicht wieder aufgebaut werden kann oder falls die Maßnahmen in einer SecureHands-Sitzung nicht erfolgreich verlaufen oder nicht das erwartete Ergebnis erzielen.
- sicherstellen, dass das/die System/e adäquat gesichert werden und, falls erforderlich, auf den letzten bekannten fehlerfreien Zustand wiederhergestellt werden können. Die Wiederherstellung des Systems liegt in der Verantwortung des Kunden.
- einen zentralen Ansprechpartner für technische Fragen benennen, der den Zugriff auf die relevanten Geräte und das Personal koordiniert.
- alle während der SecureHands-Sitzung kommunizierten oder genutzten Anmeldedaten unmittelbar nach dem Ende einer SecureHands-Sitzung zurücksetzen.

Weitere Voraussetzungen und Verantwortlichkeiten des Kunden können in der Leistungsbeschreibung vereinbart werden. Im Falle eines Konflikts zwischen diesem Dokument und der Leistungsbeschreibung gilt die Leistungsbeschreibung.

## 5.2 Verantwortlichkeiten von NTT Ltd.

### 5.2.1 Allgemeine Verantwortlichkeiten von NTT Ltd.

- NTT Ltd. ist nicht dafür verantwortlich, etwaige Änderungen an von Dritten oder dem Kunden entwickelter Hard- oder Software vorzunehmen, die in Folge eines Software-Patches oder Software-Updates notwendig sein können, das von NTT Ltd. oder dem Originalhersteller des Produkts empfohlen wird.
- NTT Ltd. ist nicht dafür verantwortlich, etwaige Änderungen an von Dritten oder dem Kunden entwickelter Hard- oder Software vorzunehmen, die notwendig sein können, um zusätzliche oder erweiterte Funktionen und Möglichkeiten nutzen zu können, die in neuen Versionen des unterstützten Produkts bereitgestellt werden.

NTT Ltd. muss

- wirtschaftlich angemessene Anstrengungen unternehmen, um die vom SOC durchgeführten Maßnahmen in ihrem Ticket-Managementsystem zu dokumentieren.
- bei der Fehlerbehebung und Diagnose mit angemessener Sorgfalt vorgehen.
- jede Fehlerbehebungssitzung im Fernzugriff in Übereinstimmung mit dem Kunden beenden, es sei denn, dass die Sitzung vom Kunden initiiert worden ist.

Zur Sicherstellung einer konsistenten Servicequalität wird das SOC:

- die vereinbarten Servicelevel überwachen.
- regelmäßige interne Serviceüberprüfungen für die kontinuierliche Serviceverbesserung durchführen.
- um Kundenfeedback bitten und Umfragen zur Kundenzufriedenheit durchführen.

**Für die Bewertung der Technologiebasis wird das SOC:**

- sicherstellen, dass alle Geräte nach der Bewertung der Technologiebasis auf den Stand vor der Bewertung zurückgesetzt werden.
- Dem Kunden nach der Bewertung die Ergebnisse der Bewertung der Technologiebasis präsentieren, und zwar in der in der Leistungsbeschreibung vereinbarten Form.



**Together we do great things**