Allgemeine Geschäftsbedingungen für die Erbringung von IT-Sicherheitsmaßnahmen durch die IS4IT KRITIS GmbH

Vorab

IS4IT KRITIS GmbH, Kraichgaublick 13, 74847 Obrigheim (nachfolgend „**IS4IT**“) ist ein hochspezialisierter Dienstleister für IT-Sicherheit. Die Erbringung der Leistungen von IS4IT unterliegt ausschließlich den nachfolgenden Allgemeinen Geschäftsbedingungen.

Sektion I.

Die Regelungen in Sektion I. kommen für jede Leistung von IS4IT zur Anwendung, die IS4IT gegenüber dem jeweiligen „**Auftraggeber**“ erbringt.

Sektion II.

Die Regelungen in Sektion II. kommen dann zur Anwendung, falls „**Phishing-Angriffe**“ Inhalt der von IS4IT zu erbringenden Leistung ist. Ein Phishing-Angriff ist der Versuch von IS4IT, über gefälschte Webseiten, E-Mails oder Kurznachrichten bzw. durch gezielte Manipulationen des Zielobjekts („**Social Engineering**“) an Zugangsdaten von vom Auftraggeber benannten Dritten (z.B. Arbeitnehmer des Auftraggebers) zu den kritischen Systemen des Auftraggebers zu gelangen. Im Erfolgsfall kann – soweit es Inhalt des Auftrags ist – IS4IT unter Verwendung der durch den Phishing-Angriff erhaltenen Zugangsdaten auf die kritischen Systeme zugreifen. Der Auftraggeber wird so in die Lage versetzt, auf menschlichem Verhalten beruhende Schwachstellen zu neutralisieren (z.B. durch Schulungen und Sensibilisierung der betroffenen Dritten) und das Risiko einer Ausnutzung dieser Schwachstellen durch einen böswilligen Angreifer zu mitigieren.

Sektion III.

Die Regelungen in Sektion III. gelten für „**Penetrationstests**“, welche die IS4IT für den Auftraggeber auf kritische Systeme durchführt. Ein Penetrationstest ist der kontrollierte Versuch von IS4IT, von innerhalb oder außerhalb der IT-Infrastruktur des Auftraggebers in eine vom Auftraggeber betriebene oder genutzte Datenverarbeitungsanlage (vorstehend und nachfolgend „**kritisches System**“) einzudringen. Laterale Bewegungen auf dem kritischen System erfolgen nicht. Hierdurch sollen Schwachstellen des kritischen Systems aufgedeckt werden. Hierbei bedient sich IS4IT unter anderem der Techniken, die nach der Expertise von IS4IT auch bei einem realen Angriff auf das kritische System angewandt werden würden. Auch der Einsatz von Vulnerability-Scannern unterliegt den Regelungen für Penetrationstests. Durch die einhergehende Identifikation der Schwachstellen des kritischen Systems wird der Auftraggeber in die Lage versetzt, die Schwachstellen zu schließen, bevor diese zum von einem Dritten in böswilliger Absicht ausgenutzt werden können.

Sektion IV.

Die in Sektion IV. enthaltenen Regelugen gelten bei für den Auftraggeber durchgeführtem „**Red Teaming“** und „**Purple Teaming“**. Beim Red Teaming wird IS4IT durch Phishing-Angriffe und/oder durch physische Angriffe und/oder der Maßnahmen eines Penetrationstests versuchen, von außen oder innen auf das kritische System zuzugreifen und dort auch laterale Bewegungen vorzunehmen, um die Schwachstellen des kritischen Systems aufzudecken. Im Gegensatz zu Penetrationstests erfolgen beim Red Teaming auch laterale Bewegungen der IS4IT auf dem kritischen System. Purple Teaming ist im Hinblick auf die Angriffsmethoden identisch zum Red Teaming; der Unterschied liegt darin, dass im Zuge des Angriffs die Verantwortlichen des Auftraggebers für IT-Sicherheit als „**Blue Team**“ eingebunden und während des Angriffes im Hinblick auf die anzuwendenden Abwehrmethoden geschult werden. Das Blue Team wird realitätsnah auf Basis der eigenen IT-Infrastruktur geschult und erlernt Strategien und Techniken zur Abwehr böswilliger Angreifer. Durch

die einhergehende Identifikation der Schwachstellen des kritischen Systems wird der Auftraggeber in die Lage versetzt, die Schwachstellen zu schließen, bevor diese von einem Dritten in böswilliger Absicht ausgenutzt werden können.

Sektion V.

Sektion V. kommt zur Anwendung, wenn IS4IT für den Auftraggeber „**physische Angriffe**“ durchführt. Ein physischer Angriff ist z.B. der Versuch, unerkannt Geschäftsräume des Auftraggebers zu betreten und die Möglichkeit eines böswilligen Angreifers aufzuzeigen, auf die dort vorhandenen Datenverarbeitungsanlagen zuzugreifen. Ein tatsächlicher Zugriff seitens IS4IT auf die Datenverarbeitungsanlagen erfolgt nicht.

Sektion I. – Allgemeine Bestimmungen

Die Regelungen in Sektion I. gelten für jede Leistungserbringung von IS4IT.

I.1. Vorrang dieser Allgemeinen Geschäftsbedingungen

I.1.1. Für die Leistungen der IS4IT kommen ausschließlich diese Allgemeinen Geschäftsbedingungen zur Anwendung. Abweichende, entgegenstehende oder ergänzende Allgemeine Geschäftsbedingungen des Auftraggebers werden nur dann und insoweit Vertragsbestandteil, als IS4IT deren Geltung ausdrücklich schriftlich zugestimmt hat.

I.2. Kritisches System und Auftragserteilung

I.2.1. IS4IT und der Auftraggeber legen schriftlich ein oder mehrere kritische Systeme des Auftraggebers fest beziehungsweise definieren den Auftrag von IS4IT schriftlich.

I.3. Einwilligung

I.3.1. IS4IT weist den Auftraggeber hin, dass dem Grunde nach die beauftragen Leistungen von IS4IT Straftaten unter anderem wegen der Verletzung des Briefgeheimnisses (§ 202 StGB), des Ausspähens von Daten (§ 202 a StGB), des Abfangens von Daten (§ 202 b StGB), des Vorbereitens des Ausspähens und Abfangens von Daten (§ 202 c StGB), der Verletzung des Post- oder Fernmeldegeheimnisses (§ 206 StGB) sowie der Datenveränderung (§ 303 a StGB) darstellen können.

In diesem Lichte willigt der Auftraggeber hiermit in Kenntnis des Auftrags ausdrücklich in die Durchführung des Auftrags durch IS4IT ein. Diese Einwilligung entfaltet ausdrücklich auch Wirkung gegenüber den von IS4IT eingesetzten Mitarbeitern und Erfüllungsgehilfen, gleich ob diese natürliche oder juristische Personen sind.

Der Auftraggeber ist im Falle polizeilicher oder staatsanwaltschaftlicher Ermittlungen verpflichtet, IS4IT zu unterstützen und die jeweiligen Ermittlungsbehörden auf die vorstehende Einwilligung hinzuweisen.

I.3.2 Wenn durch den Angriff auf das kritische System Dritte betroffen werden, ist der Auftraggeber verpflichtet, gegenüber IS4IT sämtliche betroffene Dritte zu benennen. Der Auftraggeber verpflichtet sich, die unter Ziff. I.3.1 genannte Einverständniserklärung zu Gunsten von IS4IT sowie der von IS4IT eingesetzten Mitarbeitern und Erfüllungsgehilfen von sämtlichen betroffenen Dritten einzuholen. Der Auftraggeber versichert gegenüber IS4IT ausdrücklich, diese Einwilligung vor Beginn der Leistungserbringung von IS4IT eingeholt zu haben.

I.3.3. Der Auftraggeber erlaubt IS4IT, im Rahmen der Leistungserbringung beim Auftraggeber gespeicherte personenbezogene Daten zu erheben und zu verarbeiten, zum Abruf mittels automatisierter Verfahren bereitzuhalten, abzurufen, sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien zu verschaffen und die Übermittlung an sich zu veranlassen (Erschleichen durch unrichtige Angaben). Der Auftraggeber ist verpflichtet, sicherzustellen, dass er gegenüber IS4IT alle erforderlichen Einwilligungen erteilt, um eine Strafbarkeit von IS4IT oder die Begehung einer Ordnungswidrigkeit durch IS4IT nach der Datenschutzgrundverordnung oder sonstigen Datenschutzgesetzen (z.B. BDSG) auszuschließen. Der Auftraggeber versichert, von jeder betroffenen Person i.S.v. Art. 4 Nr. 1 DS-GVO die zu vorstehend genannten Zwecken erforderlichen Einwilligungen eingeholt zu haben.

I.4. Haftung von IS4IT

I.4.1. IS4IT haftet unbeschränkt für vorsätzlich oder grob fahrlässig durch IS4IT, seine gesetzlichen Vertreter oder leitenden Angestellten verursachte Schäden sowie für vorsätzlich verursachte Schäden sonstiger Erfüllungsgehilfen; für grobes Verschulden sonstiger Erfüllungsgehilfen bestimmt sich die Haftung nach den in Ziff. I.4.5. aufgeführten Regelungen für leichte Fahrlässigkeit.

I.4.2. IS4IT haftet unbeschränkt für vorsätzlich oder fahrlässig verursachte Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit durch den Lizenzgeber, seine gesetzlichen Vertreter oder Erfüllungsgehilfen.

I.4.3. IS4IT haftet für Schäden aufgrund fehlender zugesicherter Eigenschaften bis zu dem Betrag, der vom Zweck der Zusicherung umfasst war und der für IS4IT bei Abgabe der Zusicherung erkennbar war.

I.4.4. IS4IT haftet für Produkthaftungsschäden entsprechend der Regelungen im Produkthaftungsgesetz.

I.4.5. IS4IT haftet für Schäden aus der Verletzung von Kardinalpflichten durch IS4IT, seine gesetzlichen Vertreter oder Erfüllungsgehilfen; Kardinalpflichten sind die wesentlichen Pflichten, die die Grundlage des Vertrags bilden, die entscheidend für den Abschluss des Vertrags waren und auf deren Erfüllung der Auftraggeber vertrauen darf. Wenn IS4IT diese Kardinalpflichten leicht fahrlässig verletzt hat, ist die Haftung von IS4IT auf den Betrag begrenzt, der für IS4IT zum Zeitpunkt der jeweiligen Leistung vorhersehbar war.

I.4.6. IS4IT haftet für den Verlust von Daten nur bis zu dem Betrag, der bei ordnungsgemäßer und regelmäßiger Sicherung der Daten zu deren Wiederherstellung angefallen wäre.

I.4.7. Eine weitere Haftung von IS4IT ist dem Grunde nach ausgeschlossen.

I.5. Selbstverpflichtung zur Vertraulichkeit

I.5.1. IS4IT verpflichtet sich, alle geheimhaltungsbedürftigen kaufmännischen, technischen oder sonstige unternehmensbezogene Informationen, die IS4IT während der und durch die Erfüllung des Auftrags offengelegt oder zugänglich gemacht werden, vertraulich zu behandeln und diese ausschließlich für die Zwecke der Geschäftsbeziehung zu verwenden sowie nur an diejenigen Mitarbeiter weiterzugeben, die zur Einhaltung der Vertraulichkeit verpflichtet sind. IS4IT verpflichtet sich, Vertrauliche Informationen, soweit nicht ausdrücklich etwas anderes bestimmt ist, an Dritte weder weiterzugeben noch in anderer Form zugänglich zu machen sowie alle angemessenen Vorkehrungen zu treffen, um einen Zugriff Dritter zu vermeiden.

I.5.2. Der Geheimhaltung unterliegen sämtliche Informationen, die der Auftraggeber IS4IT offenlegt oder zugänglich macht oder von denen IS4IT im Zuge der Leistungserbringung Kenntnis nimmt, die ausdrücklich als vertraulich bezeichnet sind oder auf Grund ihres Inhaltes für einen verständigen Dritten als Betriebs- oder Geschäftsgeheimnisse erkennbar sind („**Vertrauliche Informationen**“). Die Pflicht zur Geheimhaltung gilt nicht bzw. nicht mehr für Informationen, die nachweislich

(i) öffentlich zugänglich sind oder werden, ohne dass dies von IS4IT zu vertreten ist,

(ii) bei IS4IT zum Zeitpunkt der Erlangung bereits vorhanden waren oder danach von diesem unabhängig von der Übermittlung durch IS4IT erarbeitet wurden,

(iii) ohne Verletzung einer Geheimhaltungspflicht von Dritten erlangt wurden, vorausgesetzt, der Dritte verletzt nach Kenntnis von IS4IT durch die Übergabe der Informationen keine Geheimhaltungspflicht,

(iv) von IS4IT unabhängig und ohne Rückgriff auf Vertrauliche Informationen entwickelt worden sind, oder

(v) vom Auftraggeber durch schriftliche Zustimmung zur Weitergabe freigegeben wurden.

Die Darlegungslast für das Vorliegen einer der vorstehenden Ausnahmen trägt IS4IT.

I.5.4. Der Auftraggeber behält das Eigentum und alle sonstigen Rechte an den Vertraulichen Informationen, gleichgültig ob schutzfähig oder nicht. Auf Verlangen des Auftraggebers hat IS4IT die erhaltenen verkörperten Vertraulichen Informationen möglichst vollständig zurückzugeben. IS4IT kann stattdessen die Vertraulichen Informationen zerstören bzw. löschen. In diesem Fall ist die Zerstörung bzw. Löschung auf Verlangen schriftlich zu bestätigen. Diese Pflicht ist ausgeschlossen in Bezug auf Vertrauliche Informationen,

(i) gespeichert in routinemäßigen Backups,

(ii) die gemäß Gesetz, Verordnung, Urteil bzw. Beschluss eines Gerichts und/oder Anordnung einer Behörde verwahrt werden müssen oder

(iii) Vervielfältigungen von Vertraulichen Informationen, die IS4IT zu Nachweiszwecken verwahrt.

Die Geheimhaltungspflichten aus dieser Vereinbarung bleiben unberührt.

I.6. Gewerbliche Schutzrechte

I.6.1. IS4IT behält sich – soweit in diesen Allgemeinen Geschäftsbedingungen nicht ausdrücklich etwas Gegenteiliges bestimmt ist – sämtliche Schutzrechte an der von IS4IT im Rahmen der Leistungserbringung eingesetzten Software vor; insbesondere räumt IS4IT dem Auftraggeber keine Eigentumsrechte an bei der Leistungserbringung eingesetzten Software, insbesondere deren Quellcode, ein.

I.6.2. Dem Auftraggeber ist ohne vorherige schriftliche Zustimmung von IS4IT nicht berechtigt, einen von IS4IT erstellten Bericht über die im Rahmen des Auftrags gefundenen Ergebnisse (z.B. Abschlussbericht) inhaltlich abzuändern. Im Übrigen räumt IS4IT dem Auftraggeber das zeitlich und örtlich unbeschränkte Nutzungsrecht an dem von IS4IT erstellten Bericht über die im Rahmen des Auftrags gefundenen Ergebnisse ein.

I.7. Verarbeitung personenbezogener Daten

I.7.1. Soweit im Rahmen des Auftragsdurchführung von IS4IT personenbezogene Daten für den Auftraggeber verarbeitet werden, ist der Auftraggeber Verantwortlicher iSv. Art. 4 Nr. 7 DS-GVO.

I.7.2. Soweit IS4IT im Rahmen der Leistungserbringung für den Auftraggeber personenbezogene Daten verarbeitet, verpflichtet sich IS4IT diese unverzüglich nach der Leistungserbringung zu löschen.

I.8. Sonstiges

I.8.1. IS4IT ist berechtigt, die Leistungserbringung von Mitarbeitern oder sonstigen Erfüllungsgehilfen von IS4IT durchführen zu lassen.

I.8.2. Alle Vereinbarungen sind in diesem Vertrag enthalten. Die Vertragsversion in deutscher Sprache ist für diesen Vertrag maßgeblich und bindend; die englischsprachige Version dient lediglich der Veranschaulichung. Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des Kollisionsrechts und unter Ausschluss der United Nations Convention on Contracts for International Sale of Goods of 11.04.1980 (CISG).

I.8.2. Erfüllungsort ist der Sitz der IS4IT GmbH. Ausschließlicher Gerichtsstand ist München, sofern jede Partei Kaufmann oder juristische Person des öffentlichen Rechts ist.

I.8.3. Sollte eine Bestimmung dieses Vertrags oder eine künftig in ihn aufgenommene Bestimmung ganz oder teilweise unwirksam oder undurchführbar sein oder die Wirksamkeit oder Durchführbarkeit später verlieren oder sich eine Lücke herausstellen, soll hierdurch die Gültigkeit der übrigen Bestimmungen nicht berührt werden. Anstelle der unwirksamen oder undurchführbaren Bestimmung oder zur Ausfüllung der Lücke gilt eine angemessene

Regelung, die, soweit rechtlich zulässig, dem am nächsten kommt, was die Vertragsschließenden gewollt haben oder nach dem Sinn und Zweck des Vertrags gewollt hätten, falls sie den Punkt bedacht hätten.

Sektion II. – Ergänzende Regelungen für Phishing-Angriffe

Zusätzlich zu den Bestimmungen in Sektion I. gelten für von IS4IT für den Auftraggeber durchgeführte Phishing-Angriffe die nachfolgenden Regelungen.

II.1. Zielpersonen

II.1.1. IS4IT und der Auftraggeber werden vor der Durchführung des Phishing-Angriffs durch IS4IT schriftlich die Zielpersonen bzw. Gruppen von Zielpersonen sowie die kritischen Systeme festlegen. IS4IT ist verpflichtet, ausschließlich die benannten Zielpersonen anzugreifen.

II.2. Durchführung des Phishing-Angriffs

II.2.1. IS4IT ist weiter verpflichtet, die Phishing-Angriffe sorgfältig und fachmännisch auszuführen.

II.2.2. IS4IT wird im Zuge des Phishing-Angriffs den Versuch unternehmen, die Zielpersonen zur Herausgabe von Zugangsdaten zum kritischen System zu bewegen.

II.2.2. IS4IT wird – falls es bei der Erfüllung des Auftrags möglich ist – die für den Auftraggeber verarbeiteten personenbezogenen Daten der Zielpersonen und die diesbezüglich im Rahmen des Phishing-Angriffs ermittelten Ergebnisse dem Auftraggeber in anonymisierter bzw. pseudonymisierter Form übermitteln. Beim Phishing-Angriff wird IS4IT im Hinblick auf die Zielpersonen die gebotene Sorgfalt walten lassen. Insbesondere wird IS4IT keine Angriffsmethoden (z.B. Social-Engineering) einsetzten, die nach allgemeiner Lebenserfahrung dazu geeignet sind, die Psyche der Zielpersonen nachteilig zu beeinträchtigen (z.B. Androhung einer Kündigung, Aufbau psychischen Drucks, Einsatz von Schockbildern).

II.2.3. Ist ausschließlich ein Phishing-Angriff Auftragsgegenstand, ist IS4IT ohne vorherige schriftliche Gestattung des Auftraggebers nicht berechtigt, sich mit den durch den Phishing-Angriff ermittelten Zugangsdaten Zugang zu kritischen Systemen des Auftraggebers zu verschaffen. Dies gilt auch für eine Verifikation der von IS4IT ermittelten Daten.

Sektion III. – Ergänzende Regelungen für Penetrationstests

Zusätzlich zu den Bestimmungen in Sektion I. gelten für von IS4IT für den Auftraggeber durchgeführte Penetrationstests die nachfolgenden Regelungen.

III.1. Festlegung der kritischen Systeme

III.1.1. IS4IT und der Auftraggeber legen vor der Durchführung des Penetrationstests schriftlich die zu testenden kritischen Systeme fest. IS4IT verpflichtet sich, nur die vom Auftraggeber bestimmten kritischen Systeme anzugreifen.

III.2. Penetrationstest

III.2.1. IS4IT verpflichtet sich, den Penetrationstest sorgfältig und fachmännisch auszuführen. IS4IT wird das schriftlich benannte kritische System sowohl mit Vulnerability-, Scanner- und Hacking-Tools sowie mit von IS4IT entwickelten und/oder modifizierten Programmen aktiv angreifen. Die Angriffe erfolgen über öffentliche (z.B. Internet, Telefonnetz) oder sonstige Netzwerke, an die der Auftraggeber angeschlossen ist.

III.2.2. IS4IT hat den Auftraggeber über das Risiko in Kenntnis gesetzt, dass bei der Durchführung des Penetrationstests das kritische System beeinträchtigt werden kann. Insbesondere bei sog. „*Denial of Service*"-Angriffen kann es vorkommen, dass das kritische System ausfällt und als Folge hiervon gewisse Dienste zeitweise nicht mehr zur Verfügung stehen oder Daten verlorengehen. Zudem besteht das Risiko, dass Antworten der Dienste durch den Penetrationstest verzögert werden.

IS4IT wird „*Denial of Service*"-Attacken nur mit expliziter vorheriger schriftlicher Zustimmung des Auftraggebers ausführen.

III.2.3. Der Auftraggeber versichert ausdrücklich gegenüber IS4IT sowie den von IS4IT eingesetzten Mitarbeitern und Erfüllungsgehilfen, dass die kritischen Systeme, die vom Auftraggeber gem. Ziff. III.1.1. schriftlich benannt wurden, ausschließlich vom Aufraggeber betrieben und genutzt werden und Dritte von einer Beeinträchtigung der gegenständlichen kritischen Systeme oder mit diesen verbundenen Systemen nicht betroffen werden. Werden die gegenständlichen kritischen Systeme nicht exklusiv durch den Auftraggeber genutzt oder werden mit den kritischen Systemen verbundene Systeme von Dritten genutzt, versichert der Auftraggeber ausdrücklich, dass er sämtliche Einwilligungen der betroffenen Dritten für einen Penetrationstest des gegenständlichen kritischen Systems eingeholt hat, die betroffenen Dritten über die möglichen Auswirkungen des Penetrationstests belehrt hat und die betroffenen Dritten in die Durchführung des Penetrationstests eingewilligt haben. Widersprechen betroffene Dritte gegenüber IS4IT dem Penetrationstest auf das gegenständliche kritische System, ist IS4IT berechtigt, den Penetrationstest dieses kritischen Systems unverzüglich einzustellen. Der Auftraggeber hat für den hierdurch entstehenden Schaden einzustehen. Der Auftraggeber hält IS4IT vollumfänglich schadlos, sollte IS4IT von Dritten in Anspruch genommen werden, weil der Auftraggeber die erforderlichen Zustimmungen Dritter nicht rechtzeitig eingeholt hat und/oder wenn durch den Penetrationstest des kritischen Systems Schäden bei Dritten entstehen. Dies gilt auch für Schäden, welche Dritten aufgrund der Beeinträchtigung von mit dem kritischen System verbundenen Systemen entstehen. Diese Pflicht zur Schadloshaltung entfällt bei grob fahrlässigem oder vorsätzlichem Handeln von IS4IT, Vertretern oder Erfüllungsgehilfen von IS4IT oder bei Verletzung von Kardinalpflichten der IS4IT.

III.3. Grenzen des Penetrationstests

III.3.1. IS4IT wird den Penetrationstest unverzüglich zu unterbrechen, sobald für IS4IT erkennbar ist, dass durch den Penetrationstest eine nachhaltige Beschädigung einer für den Auftraggeber kritischen Infrastruktur möglich ist. IS4IT wird den Auftraggeber unverzüglich auf den Abbruch des Angriffes hinweisen. IS4IT wird erst mit vorheriger

schriftlicher Zustimmung des Auftraggebers den Penetrationstest auf das gegenständliche kritische System weiter fortsetzen.

III.3.2. Sofern und soweit IS4IT im Rahmen des Penetrationstests auf personenbezogene Daten von betroffenen Personen (z.B. Vertragspartner oder Mitarbeitern des Auftraggebers) stößt, die eindeutig deren privaten Lebensbereich zuzuordnen sind, wird IS4IT entsprechend der Regelungen in Ziffer III.3.1. vorgehen.

Sektion IV. – Ergänzende Regelungen für Red Teaming und Purple Teaming

Zusätzlich zu den Bestimmungen in Sektion I., Sektion II. und Sektion III. gelten für von IS4IT für den Auftraggeber durchgeführtes Red Teaming oder Purple Teaming die nachfolgenden Regelungen.

IV.1. Angriffsmittel

IV.1.1. Der Umfang der Angriffsmittel aus Ziffer. III.2.1. wird dahingehend erweitert, dass bei einem Phishing-Angriff auch Computerprogramme („**Trojaner**“), die ohne Wissen der Zielperson eine andere Funktion erfüllen als sie vorgeben (z.B. Rootkits), auf den Endgeräten der Zielpersonen platziert und betrieben werden können. Ebenso ist IS4IT berechtigt, sich Zugang zu vom Auftraggeber schriftlich bezeichneten Geschäftsräumen des Auftraggebers zu verschaffen.

IV.2. Hauptverantwortlicher; Blue Team und Purple Team; Gesetzliche Vorschriften

IV.2.1. Spätestens 10 Werktage vor Beginn der Leistungserbringung von IS4IT hat der Auftraggeber schriftlich einen auf Seiten des Auftraggebers hauptverantwortlichen Ansprechpartner gegenüber IS4IT zu benennen. Der Auftraggeber stellt sicher, dass der hauptverantwortliche Ansprechpartner im Zeitraum der Leistungserbringung durchgehend erreichbar ist. Weiter stellt der Auftraggeber sicher, dass der hauptverantwortliche Ansprechpartner gegenüber IS4IT wie auch sonstigen Dritten für und wider den Auftraggeber in einem solchen Umfang bindende Willenserklärungen abgeben darf, dass er im Innen- wie im Außenverhältnis gegenüber IS4IT oder sonstigen Dritten hinsichtlich der Leistungserbringung bindende und wirksame Anordnungen treffen kann. Dies umfasst auch das Hausrecht für die Geschäftsräume des Auftraggebers.

IV.2.2. Falls das Red Teaming von IS4IT durch ein Blue Team des Auftraggebers (z.B. Mitarbeiter oder Erfüllungsgehilfen des Auftraggebers, welche im Zuge des Angriffes Abwehrmaßnahmen gegen den Angriff der IS4IT erörtern, planen oder einleiten sollen) begleitet wird (Purple Teaming), sind das Blue Team der IS4IT spätestens 10 Werktage vor Beginn der Leistungsausführung schriftlich zu benennen.

IV.2.3. Der Auftraggeber versichert, dass er vor Beginn des Red Teamings bzw. des Purple Teamings der IS4IT das im Rahmen von Ziff. IV.2.1. eingesetzte Blue Team darüber belehrt hat, dass die von IS4IT eingesetzten und vermittelten Techniken ohne eine ausdrückliche Einwilligung der natürlichen oder juristischen Person, in deren Eigentum bzw. Verfügungsgewalt das kritische System steht, einen Verstoß gegen strafrechtliche Vorschriften darstellen.

IV.3. Physischer Angriffe; Schriftliches Betretungsrecht

IV.3.1. Ist eine Zugangsverschaffung i.S.v. Ziff. IV.1.1. Leistungsgegenstand, erteilt der Auftraggeber IS4IT die Erlaubnis, die vom Auftraggeber schriftlich bezeichneten Geschäftsräume des Auftraggebers während oder außerhalb der Geschäftszeiten des Auftraggebers zu betreten, sich hierin aufzuhalten und auf die hierin vom Auftraggeber vorgehaltene IT-Infrastruktur, hierin befindliche Endgeräte und das kritische System einzuwirken („**physisches Red Teaming**“).

IV.3.2. Der Auftraggeber wird IS4IT beziehungsweise den von IS4IT benannten Mitarbeitern oder sonstigen Erfüllungsgehilfen die schriftliche Bestätigung einer für den Auftraggeber vertretungsberechtigten Person, die ebenfalls über das Hausrecht der gegenständlichen Geschäftsräume disponieren kann, über das Recht zum physischen Red Teaming ausstellen. Die schriftliche Bestätigung muss zur Vorlage gegenüber Dritten, insbesondere private Sicherheitsunternehmen oder Strafverfolgungsbehörden (z.B. Polizei, Staatsanwaltschaft) bestimmt sein und den Aussteller der Bestätigung sowie den Umfang der eingeräumten Rechte klar und eindeutig erkennen lässt.

IV.3.3. Soweit das physische Red Teaming das Betreten von bzw. den Aufenthalt in befriedetem Besitztum (Gebäude oder Freiflächen), das nicht ausschließlich in der Herrschaftsgewalt des Auftraggebers steht, erfordert, versichert der Auftraggeber ausdrücklich, sämtliche erforderlichen Einwilligungen von Dritten zu Gunsten von IS4IT sowie den von IS4IT eingesetzten Mitarbeitern und sonstigen Erfüllungsgehilfen eingeholt zu haben, die erforderlich sind, damit IS4IT bzw. Mitarbeiter oder sonstige Erfüllungsgehilfen von IS4IT ohne die Verletzung von Eigentums- bzw. Besitzrechten Dritter das physische Red Teaming durchführen können.

Sektion V – Ergänzende Regelungen für physische Angriffe

Zusätzlich zu den Bestimmungen in Sektion I. gelten für von IS4IT für den Auftraggeber durchgeführte Physische Angriffe die nachfolgenden Regelungen.

V.1.1. Der Auftraggeber erteilt IS4IT die Erlaubnis, die vom Auftraggeber schriftlich bezeichneten Geschäftsräume des Auftraggebers während oder außerhalb der Geschäftszeiten des Auftraggebers zu betreten und sich hierin aufzuhalten. IS4IT wird nicht auf die vom Auftraggeber vorgehaltene IT-Infrastruktur, sich in den Geschäftsräumen befindliche Endgeräte oder das kritische System einzuwirken.

V.1.2. Der Auftraggeber wird IS4IT beziehungsweise den von IS4IT benannten Mitarbeitern oder sonstigen Erfüllungsgehilfen die schriftliche Bestätigung einer für den Auftraggeber vertretungsberechtigten Person, die ebenfalls über das Hausrecht der gegenständlichen Geschäftsräume disponieren kann, über das Recht zum physischen Angriff ausstellen. Die schriftliche Bestätigung muss zur Vorlage gegenüber Dritten, insbesondere private Sicherheitsunternehmen oder Strafverfolgungsbehörden (z.B. Polizei, Staatsanwaltschaft) bestimmt sein und den Aussteller der Bestätigung sowie den Umfang der eingeräumten Rechte klar und eindeutig erkennen lässt.

V.1.3. Soweit der physische Angriff das Betreten von bzw. den Aufenthalt in befriedetem Besitztum (Gebäude oder Freiflächen), das nicht ausschließlich in der Herrschaftsgewalt des Auftraggebers steht, erfordert, versichert der Auftraggeber ausdrücklich, sämtliche erforderlichen Einwilligungen von Dritten zu Gunsten von IS4IT sowie den von IS4IT eingesetzten Mitarbeitern und sonstigen Erfüllungsgehilfen eingeholt zu haben, die erforderlich sind, damit IS4IT bzw. Mitarbeiter oder sonstige Erfüllungsgehilfen von IS4IT ohne die Verletzung von Eigentums- bzw. Besitzrechten Dritter den physischen Angriff durchführen können.