



Inhaltsverzeichnis

1	Allgemeine Anforderungen.....	2
1.1	Offenlegungspflichten	2
1.2	Informationspflichten.....	3
1.3	Sorgfaltspflichten	5
2	Anforderungen aus dem Security Framework	6
2.1	Sichere Software-Entwicklung.....	6
2.2	Identity und Access Management	7
2.3	Anforderungen zu Business Continuity.....	8
2.4	Anforderungen zu Training und Awareness.....	9
3	Anforderungen zur Arbeitssicherheit & Gesundheitsschutz (Safety).....	9
3.1	Schutz von Leben und Förderung der Gesundheit	9
3.2	Verpflichtungen zur Einhaltung der Safety-Regeln	9
3.3	Spezifische Safety-Verpflichtungen des Lieferanten.....	9
3.4	Weisungs- und Einsichtsbefugnisse von Swisscom	10
4	Fristen.....	10
5	Kontaktpersonen und Kommunikation	11
5.1	Kontaktpersonen beim Lieferanten.....	11
5.2	Notfallkontakt Swisscom	11

1 Allgemeine Anforderungen

Die folgenden Anforderungen basieren auf dem ISO27001:2013 Standard und den Anforderungen aus dem Security Framework der Swisscom. Insoweit untenstehende Sicherheitsvorgaben auf den Vertragsgegenstand anwendbar sind, verpflichtet sich der Lieferant, diese als minimale Sicherheitsvorgaben während der gesamten Vertragsdauer einzuhalten.

1.1 Offenlegungspflichten

1.1.1 Allgemeine Offenlegungspflicht

Der Lieferant verpflichtet sich, die im Kontext der angestrebten Geschäftsbeziehung für die Sicherheit relevanten Dokumente und Informationen offenzulegen. Dies betrifft insbesondere, aber nicht ausschliesslich, technische Unterlagen wie Architekturen, funktionale Konzepte, Kommunikationsmatrizen und Sicherheitskonzepte. Swisscom wird ihrerseits alle Unterlagen zur Verfügung stellen, die der Lieferant zur Erfüllung seiner Aufgaben im Rahmen der Vorhaben benötigt.

1.1.2 Auditrecht

Der Lieferant verpflichtet sich, auf Anfrage der Swisscom den Umgang mit Security und Safety im eigenen Unternehmen, soweit es für die Geschäftsbeziehung notwendig ist, offenzulegen. Der Lieferant sichert Swisscom hierfür ein Auditrecht bei sich selbst und bei Unterlieferanten zu. Swisscom wird dabei die eigenen Kosten selbst tragen. Swisscom stellt den Auditantrag schriftlich an die Kontaktstelle des Lieferanten mit folgendem Inhalt:

- auditiertes Bereich,
- zu überprüfende Systeme, Verfahren, Abläufe und Dokumente,
- gewünschter Termin,
- Auditteam.

Das detaillierte Auditprogramm wird von Swisscom erstellt und zwischen den Parteien vereinbart. Der Lieferant unterstützt Swisscom vollumfänglich bei der Durchführung solcher Audits. Diese Unterstützung beinhaltet unter anderem die Offenlegung von Logdateien (inklusive ggf. notwendiger Werkzeuge zur Analyse dieser Dateien) und die Gewährung benötigter Zugriffsrechte. Dabei sind Systeme, Verfahren, Werkzeuge, Abläufe und Dokumente, welche dem Auditteam nicht zugänglich sind, aufzuzeigen. Der Lieferant gewährleistet die Durchführbarkeit gemäss Auditprogramm. Das Auditteam wird durch Vertreter des Lieferanten begleitet. Swisscom kann Dritte mit der Durchführung von Audits beauftragen. Die von Swisscom beauftragten Dritten unterstehen einer Vertraulichkeitsverpflichtung gegenüber dem Lieferanten und Swisscom.

Swisscom informiert den Lieferanten über die Ergebnisse des Audits. Die Aufwände des Lieferanten zur Durchführung des Audits trägt der Lieferant selbst (z.B. Anreise, Arbeitszeit und Spesen der im Rahmen des Audits lieferantenseitig befragten Personen, Bereitstellung von Dokumenten, etc.).

Ohne begründeten Anlass wird Swisscom keine Audits durchführen. Als begründeter Anlass gelten namentlich auch Auditanforderungen aufgrund gesetzlicher und regulatorischer Vorgaben seitens der



Kunden von Swisscom oder deren Aufsichtsbehörden, soweit diese die Leistungen des Lieferanten ebenfalls betreffen, oder die Qualität in Bezug auf die vereinbarten Sicherheitsvorkehrungen.

1.1.3 Rückgabe Swisscom Assets

Der Lieferant verpflichtet sich, sämtliche zur Verfügung gestellten Arbeitsmittel der Swisscom nach Beendigung der Geschäftsbeziehung kurzfristig (Fristen: siehe 4) und unaufgefordert zurückzugeben. Die Zutrittsmittel sind nach Beendigung des Vertragsverhältnisses unaufgefordert der Kontaktperson bei Swisscom zurückzugeben.

Bei Verlust eines Zutrittsmittels ist die Kontaktperson gemäss Vertrag sofort zu informieren. Sollte dies nicht möglich sein, ist das Swisscom PCard Center direkt zu kontaktieren über Center-Swisscom.PCard@swisscom.com. Bei Verlust einer Partner Card schuldet der Lieferant für Material und Umtriebe eine Entschädigung von CHF 500.--.

1.1.4 Nichtflüchtige Speichermedien

Im Rahmen des Auftrags eingesetzte nichtflüchtige Speichermedien werden bei Defekt zur Wahrung der Vertraulichkeit darauf enthaltener Informationen durch Swisscom unlesbar vernichtet (geschreddert) und entsorgt. Dies gilt auch für Medien, für die noch eine Gewährleistungspflicht besteht.

Am Nutzungsende von nichtflüchtigen Speichermedien werden diese mit sicheren Lösungsverfahren gelöscht oder von Swisscom vernichtet (geschreddert) und entsorgt.

Im Rahmen des Auftrags eingesetzte nichtflüchtige Speichermedien des Lieferanten müssen nach Beendigung des Auftrags sicher und nachweislich gelöscht werden. Falls dies technisch nicht möglich ist, müssen diese Speichermedien vernichtet (geschreddert) werden.

Der Restwert der vernichteten Speichermedien wird dem Lieferanten auf Anfrage erstattet.

1.2 Informationspflichten

1.2.1 Einhaltung der Sicherheitsanforderungen

Der Lieferant verpflichtet sich die vereinbarten Lieferobjekte gemäss Stand der Technik zu sichern. Swisscom behält sich vor, im Einzelfall detailliertere Sicherheitsvorgaben in den individuellen Vorhaben zu vereinbaren. Der Lieferant verpflichtet sich eine vorhabenspezifische Konformitätserklärung als Bestandteil des Angebots abzugeben, in der er allfällige Abweichungen offenlegt und begründet. Dies gilt für alle Sicherheitsanforderungen unabhängig von ihrer Kritikalität.

1.2.2 Qualität der Lieferobjekte

Sämtliche vom Lieferanten bereitgestellten Lieferobjekte müssen zum Zeitpunkt der Bereitstellung frei von bekannten Schwachstellen sein. Falls dies nicht möglich ist, sind die bekannten Schwachstellen vollständig zu dokumentieren und Swisscom mitzuteilen. Der Lieferant stellt sicher, dass sämtliche Komponenten des Lieferobjekts, einschliesslich Komponenten von Drittanbietern, diese Anforderung erfüllen.

1.2.3 Dokumentation der Sicherheit des Lieferobjekts

Der Lieferant stellt eine Dokumentation zur Verfügung, welche die sicherheitsrelevanten Parameter des Lieferobjekts vollständig beschreibt.

1.2.4 Information bei Sicherheitsvorfällen



Die Sicherheitsorganisationen von Swisscom und dem Lieferanten werden sich bei Sicherheitsvorfällen, welche den entsprechenden Lieferantenvertrag betreffen, sofort (Fristen siehe 4) gegenseitig informieren. Der Lieferant verpflichtet sich Swisscom unverzüglich (Fristen: siehe 4) über sicherheitsrelevante Vorfälle zu informieren, falls diese Vorfälle eine Auswirkung auf die Geschäftsbeziehungen bzw. Geschäftsgegenstände von Swisscom haben, bevor diese Informationen der Öffentlichkeit zuteilwerden.

1.2.5 Information über Weiterentwicklung im Bereich Security

Der Lieferant verpflichtet sich, Swisscom über Veränderungen im Sicherheitsdispositiv seiner Lieferobjekte (soweit Swisscom betreffend) zu informieren, bevor diese Informationen der Öffentlichkeit zuteilwerden. Dies betrifft auch Komponenten, die von Sublieferanten entwickelt wurden. Diese Informationen werden von Swisscom vertraulich behandelt.

1.2.6 Schwachstellen in Produkten

Der Lieferant verpflichtet sich, Swisscom über sicherheitsrelevante Schwachstellen seiner Lieferobjekte inkl. Komponenten von Drittlieferanten und die geplanten Massnahmen zur Behebung dieser sicherheitsrelevanten Schwachstellen (inkl. Roadmap, verfügbare Patches und Updates etc.) zu informieren, bevor diese Informationen der Öffentlichkeit zuteilwerden. Diese Informationen werden von Swisscom vertraulich behandelt. Der Lieferant verpflichtet sich ferner, Swisscom unverzüglich (Fristen: siehe 4) nach Verfügbarkeit, Updates, Patches etc. zur Behebung der sicherheitsrelevanten Schwachstelle kostenfrei zur Verfügung zu stellen.

1.2.7 Kryptographische Verfahren

Werden im Lieferobjekt kryptographische Verfahren angewendet, so müssen diese durch den Lieferanten ausgewiesen und dokumentiert werden. Es dürfen ausschliesslich kryptographische Verfahren zum Einsatz kommen, die zum Zeitpunkt der Bereitstellung des Lieferobjekts nicht als erfolgreich angreifbar bekannt sind. Es sind kryptographische Verfahren vorzuziehen, deren Implementierung durch unabhängige Dritte (z.B. Deutsches BSI) verifizierbar sind bzw. als sicher eingestuft sind.

1.2.8 Identifikation von beauftragten Personen

Der Lieferant stellt sicher, dass zur Auftragserfüllung eingesetzte Personen, die nicht öffentlich zugängliche Einrichtungen von Swisscom betreten müssen, eine sichtbare persönliche Identifizierungsmöglichkeit mit sich führen und auf Verlangen vorweisen. Solche sichtbaren Identifizierungsmöglichkeiten werden, falls notwendig, von Swisscom zur Verfügung gestellt. Grundsätzlich werden personalisierte Zutrittskarten abgegeben. Der Lieferant stellt sicher, dass bei ausnahmsweiser Verwendung von unpersönlichen Zutrittsmitteln jederzeit nachweisbar ist, welche Einzelperson zu welcher Zeit das Zutrittsmittel verwendet hat. Bei einer erheblichen Anzahl benötigter Zutritte kann der Lieferant nach entsprechender Prüfung als "Trusted Access Partner" anerkannt werden, um das Management der Zutrittskarten zu vereinfachen.

1.2.9 Persönliche Vertraulichkeitserklärung

Swisscom ist berechtigt, von Personen, denen der Zugang und Zugriff auf Services oder Daten von Swisscom eingeräumt werden soll, vor Erteilung einer Zugangs- oder Zugriffsberechtigung die

Unterzeichnung einer Vertraulichkeitserklärung zu verlangen. Personen, welche sich weigern die Vertraulichkeitserklärung zu unterzeichnen, dürfen von Swisscom abgelehnt werden.

1.2.10 EINFORDERUNG STRAFREGISTERAUSZUG UND BETREIBUNGSREGISTERAUSZUG

Swisscom ist berechtigt, von Personen, denen von Swisscom Zugang und Zugriff auf Services oder auf Swisscom-Daten (Daten von Swisscom selber und/oder Daten, die Swisscom im Auftrag Dritter bearbeitet) eingeräumt werden soll, vor Erteilung der Zugriffsberechtigung über den Lieferanten einen Strafregisterauszug und einen Betriebsregisterauszug zu verlangen. Personen, welche die Aushändigung eines Strafregisterauszuges und/oder des Betriebsregisterauszuges verweigern oder einen Registereintrag haben, durch den das Vertrauen in die Person beeinträchtigt ist, dürfen von Swisscom abgelehnt werden.

1.2.11 ZUSÄTZLICHE SICHERHEITSPRÜFUNGEN

Insoweit die Kunden von Swisscom zusätzliche Sicherheitsprüfungen verlangen, ist Swisscom berechtigt, diese Sicherheitsprüfung auch von den vom Lieferanten zur Auftragserfüllung eingesetzten Personen zu verlangen. Personen, welche sich weigern sich diesen zusätzlichen Sicherheitsprüfungen zu unterziehen oder diese nicht erfüllen, dürfen von Swisscom abgelehnt werden

1.3 Sorgfaltspflichten

1.3.1 Verfolgung der aktuellen Entwicklungen

Der Lieferant verpflichtet sich, Weiterentwicklungen auf dem Gebiet der Security und Safety laufend zu verfolgen, und seine Produkte entsprechend dem Stand der Wissenschaft und Technik fortlaufend zu verbessern.

1.3.2 Weitergabe Sicherheitsanforderungen an Sublieferanten

Im Fall des Beizugs genehmigter Subunternehmen oder Sublieferanten stellt der Lieferant sicher, dass die von den Sublieferanten zur Auftragserfüllung eingesetzten Personen über die Sicherheitsanforderungen von Swisscom informiert sind und diese verstehen und dass die Sicherheitsanforderungen von Swisscom von diesen Personen eingehalten werden. Der Lieferant ist vollumfänglich für die richtige Auswahl, Instruktion und Überwachung der für die Auftragserfüllung eingesetzten Personen verantwortlich und haftet für deren Fehlverhalten wie für ein eigenes Fehlverhalten.

1.3.3 Sicherheitsmassnahmen des Lieferanten

Der Lieferant stellt sicher, dass die Systeme, welchen zur Auftragserfüllung der Zugriff auf eines der Netze der Swisscom eingeräumt wird, in seiner Verantwortung stehen und den anerkannten, allgemeinen Sicherheitsstandards entsprechen. Der Lieferant bezeichnet auf Anfrage die angewendeten Standards, legt bestehende vertiefende Publikationen offen und erbringt entsprechende Nachweise. Dies gilt sowohl für Arbeitsplatzrechner als auch für Support Systeme für z.B. Wartung, Test und Deployment (lokaler und/oder remote Zugriff).

1.3.4 Umgang mit Assets



Swisscom und der Lieferant stellen sicher, dass mit Arbeitsmitteln des Vertragspartners umsichtig umgegangen wird, um unbefugten physischen Zutritt, Beschädigung und Beeinträchtigungen der Einrichtungen und Daten zu verhindern. Dies beinhaltet auch, dass Ausrüstungsteile, Informationen oder Hard-/ Software nicht ohne die vorherige Ermächtigung durch Swisscom oder den Eigentümer entfernt oder entsorgt werden dürfen.

1.3.5 Schutz der Arbeitsgeräte des Lieferanten

Der Lieferant stellt sicher, dass alle Geräte, mit denen der Zugriff auf Swisscom-Daten oder Services von Swisscom erfolgen soll, dem Stand der Technik hinsichtlich Schutzmechanismen (Antimalware, Patch Management, Passwort-Sicherheit, Logging, Netzwerksicherheit, etc.) entsprechen. Die getroffenen Massnahmen sind zu dokumentieren. Geräte und Systeme des Lieferanten müssen vor einem Anschluss an die Netzwerkinfrastruktur oder ICT-Einrichtungen von Swisscom autorisiert werden.

1.3.6 Prüfung der Arbeitsgeräte mit Zugriff auf Assets von Swisscom

Swisscom behält sich vor, die Arbeitsgeräte des Lieferanten, über welche Zugriffe auf Swisscom Daten oder Services erfolgen, auf die Einhaltung der unter 1.3.5 definierten Anforderungen zu prüfen. Geräte, die den Anforderungen nicht entsprechen, dürfen nicht verwendet werden.

1.3.7 Bild- und Tonaufnahmen

Bild- und Tonaufzeichnungen jeglicher Art (Foto-, Video- oder Fernsehaufnahmen etc.) sind grundsätzlich untersagt, sofern diese nicht im Rahmen der schriftlichen Beauftragung explizit verlangt (z.B. Werksabnahmen) wurden oder der von Swisscom autorisierten Beweissicherung dienen. Diese Aufnahmen dürfen nur im Rahmen des Zwecks der Leistungserbringung eingesetzt werden, eine Veröffentlichung von Bild- und Tonaufzeichnungen ist nicht erlaubt. Soll dies in einem Einzelfall trotzdem erfolgen, muss in jedem Fall vorgängig das Einverständnis von Swisscom eingeholt werden. Der Lieferant wendet sich zu diesem Zweck an seine Kontaktperson laut Vertrag.

1.3.8 Weitergabe von Daten und Umgang mit Daten

Der Lieferant hat bei der Bearbeitung von Swisscom-Daten grundsätzlich die gleichen Sicherheitsvorgaben einzuhalten, die Swisscom selbst verwendet. Der Lieferant ist nicht befugt, Swisscom Daten ohne vorherige Genehmigung von Swisscom an Dritte weiterzugeben oder zu anderen Zwecken als zur Vertragserfüllung zu verwenden.

2 Anforderungen aus dem Security Framework

2.1 Sichere Software-Entwicklung

2.1.1 Grundsatz der sicheren Softwareentwicklung

Der Lieferant stellt sicher, dass eine allfällig geschuldete Softwareentwicklung unter Beachtung der Grundsätze sicherer Softwareentwicklung erfolgt.

2.1.2 Ausbildung zur sicheren Software-Entwicklung



Der Lieferant stellt darüber hinaus sicher, dass die mit der Softwareentwicklung für Swisscom betrauten Mitarbeitenden eine gute Kenntnis sicherheitsrelevanter Aspekte der Softwareentwicklung haben und diese in regelmässigen Weiterbildungen erhalten und vertiefen.

2.1.3 Spezifikation für sicherheitsrelevante Software

Der Lieferant stellt sicher, dass die sicherheitsrelevanten Bestandteile der entwickelten Software spezifiziert und getestet sind. Auf Anfrage von Swisscom stellt der Lieferant die Spezifikation der sicherheitsrelevanten Bestandteile, die Ergebnisse der Tests dieser Bestandteile sowie die zugehörigen Test Cases zur Verfügung.

2.1.4 Sicherheitsrelevante Tests

Der Lieferant führt kontinuierlich sicherheitsrelevante Tests der entwickelten Software durch. Der Lieferant stellt auf Anfrage von Swisscom die Testresultate zur Verfügung.

2.1.5 Test ohne Echtdaten

Der Lieferant stellt sicher, dass Tests der entwickelten Software auch ohne die Bereitstellung von Echtdaten durchgeführt werden können. Die Nutzung von anonymisierten bzw. pseudonymisierten Testdaten ist in jedem Fall vorzuziehen. Abweichungen davon genehmigt Swisscom nur aufgrund der Umstände des Einzelfalls mittels einer expliziten Ausnahmegenehmigung. Sollte der Einsatz von Echtdaten unabdingbar sein und werden dem Lieferanten für Testzwecke Echtdaten von Swisscom zur Verfügung gestellt, so ist der Lieferant in der Pflicht, die Echtdaten zu jedem Zeitpunkt angemessen zu schützen. Dies betrifft vor allem Speicherung, Transport, Umgang mit, Zugriff auf und Entsorgung der Daten. Die vollständige Entsorgung der Daten wird Swisscom nach Beendigung des Tests bestätigt. Swisscom hat das Recht, dies nachprüfen zu lassen. Der Lieferant stellt darüber hinaus sicher, jederzeit vollumfänglich über Einsatz von Zugriff auf und Speicherung der Echtdaten Auskunft erteilen zu können.

2.2 Identity und Access Management

Greift der Lieferant im Rahmen seine Leistungserbringung auf Daten oder Services von Swisscom zu, verpflichtet sich der Lieferant zusätzlich nachfolgende Bestimmungen einzuhalten:

2.2.1 Zugriffe über bewilligte Verfahren

Zugang und Zugriff auf Systeme und das Netzwerk von Swisscom sind ausschliesslich unter Verwendung der von Swisscom explizit bewilligten oder akzeptierten Zugriffswege und Zugriffsmittel gestattet.

2.2.2 Personalisierte Zugriffe auf Systeme und Zutritte in Gebäude

Zugriffe auf Systeme von Swisscom oder deren Kunden darf ausschliesslich durch Personen erfolgen, die Swisscom namentlich bekannt gegeben wurden. Der Lieferant hat jeweils anzugeben, ob es sich um eigene Mitarbeitende oder, sofern zulässig, um Mitarbeitende von Dritten handelt.

Der Zutritt in Gebäude von Swisscom oder von deren Kunden darf ausschliesslich durch Personen erfolgen, die Swisscom namentlich bekannt gegeben wurden. Der Lieferant hat jeweils anzugeben, ob es sich um eigene Mitarbeitende oder, sofern zulässig, um Mitarbeitende von Dritten handelt.

Der Zutritt von Personen des Lieferanten zu Gebäuden oder Teilen von Gebäuden von Swisscom oder deren Kunden kann von Swisscom eingeschränkt werden.



2.2.3 Verbotene Gateway Funktionen

Der Lieferant stellt sicher, dass ein mit dem Netzwerk von Swisscom verbundenes Gerät des Lieferanten nicht als „Sprungbrett“/Gateway missbraucht werden kann. Das entsprechende Gerät darf im Moment des Fernzugriffs keine weiteren Netzwerkverbindungen unterhalten; dies ist durch technische und/oder organisatorische Massnahmen sicherzustellen.

2.2.4 Sicherheitsmechanismen für Remotezugang

Security Tokens und andere Sicherheitsmechanismen zur Authentisierung dürfen nie an andere Personen weitergegeben werden, es sei denn, die Weitergabe ist explizit vertraglich geregelt (z.B. internationale Support-Organisationen). Bei Verlust von Security Tokens oder anderen Sicherheitsmechanismen informiert der Lieferant unmittelbar bei Entdeckung (Fristen: siehe 4), damit Swisscom entsprechende Sperrmassnahmen treffen kann.

2.2.5 Änderung bei beauftragtem Personal

Der Lieferant ist verpflichtet, nicht mehr benötigte Benutzeraccounts oder Zugriffs- / Zutrittsberechtigungen Swisscom umgehend (Fristen: siehe 4) zu melden, damit Swisscom die notwendigen Vorkehren umgehend treffen kann. Nicht mehr benötigte Zutrittsmittel oder Zugriffsmittel müssen retourniert werden.

2.2.6 Austritt bei beauftragtem Personal

Der Lieferant ist verpflichtet, Swisscom sofort darüber in Kenntnis zu setzen, wenn das Arbeits- oder Auftragsverhältnis mit einer zugriffs- oder zutrittsberechtigten Person aufgelöst oder die Person von ihrem Dienst suspendiert wird oder nicht mehr im Einsatz für Swisscom steht. Swisscom ist berechtigt, den Einsatz von Personen in gekündigtem Arbeits- oder Auftragsverhältnis abzulehnen und den entsprechenden Zugang zu sperren.

2.2.7 Dauer der Verbindung

Verbindungen ins Netzwerk von Swisscom sind zu trennen, sofern die Art der Verbindung eine Trennung erlaubt, wenn die Verbindung länger als 30 Minuten nicht benötigt wird oder am Ende von jedem Arbeitstag. Nach Abschluss der vertraglich geschuldeten Leistungen ist die Verbindung auf jeden Fall zu trennen.

2.2.8 Auslandszugriffe

Zugriffe aus dem Ausland sind nur in definierten Ausnahmefällen zulässig und bedürfen vorgängig einer Bewilligung durch Swisscom. Die dabei verwendeten Verfahren und Prozesse sind zu dokumentieren und von Swisscom zu genehmigen.

2.3 Anforderungen zu Business Continuity

2.3.1 Dokumentation Business Continuity Anforderungen

Der Lieferant stellt die Dokumentation zur Verfügung, welche hinsichtlich der Lieferobjekte für die Erstellung von Wiederanlaufplänen benötigt werden.

2.3.2 Notfall- und Krisenmanagement Lieferant

Der Lieferant verpflichtet sich, auf Anfrage seine Notfall- und Krisenorganisation aufzuzeigen und bei Bedarf geeignete Schnittstellen zum Krisenmanagement Swisscom zu schaffen. Bei Bedarf kann er im Krisenfall als Fachstab zur Krisenorganisation Swisscom beigezogen werden.

2.4 Anforderungen zu Training und Awareness

2.4.1 Ausbildung in Bezug auf neue Gefahren

Der Lieferant verpflichtet sich, Weiterentwicklungen auf dem Gebiet der Informationssicherheit kontinuierlich zu verfolgen und seine Mitarbeitenden entsprechend auszubilden. Dies gilt im Besonderen für den Gegenstand der Geschäftsbeziehung zwischen Swisscom und dem Lieferanten.

2.4.2 Spezifische Awareness Schulung

Der Lieferant stellt sicher, dass alle Mitarbeitenden des Lieferanten mit Zutritt oder Zugriff auf Swisscom Daten oder Services eine Basisschulung in Bezug auf die Sicherheit und Safety erhalten. Die Aufwände hierfür können Swisscom nicht in Rechnung gestellt werden. Swisscom wird auf Anfrage Vertretern des Lieferanten weitere Schulungen über die Sicherheitsvorgaben von Swisscom ermöglichen. Der Lieferant verpflichtet sich im Gegenzug, Vertretern der Swisscom Schulungen über die sicherheitsrelevanten Eigenschaften des Gegenstands der Geschäftsbeziehung zu ermöglichen.

3 Anforderungen zur Arbeitssicherheit & Gesundheitsschutz (Safety)

3.1 Schutz von Leben und Förderung der Gesundheit

Die Abteilung Safety bei Swisscom bemüht sich, die physische wie die psychische Gesundheit der Arbeitnehmenden zu fördern und zu beschützen. Mit Blick auf dieses Grundprinzip muss der Lieferant alle notwendigen Massnahmen umsetzen, um das Leben und die Gesundheit seiner bei Swisscom tätigen Mitarbeitenden sowie der Mitarbeitenden und Kunden von Swisscom zu schützen.

3.2 Verpflichtungen zur Einhaltung der Safety-Regeln

Gemäss Art. 3 und 9 der Verordnung über die Unfallverhütung (VUV, SR 832.30) sowie Art. 3 Bauarbeitenverordnung (BauAV; 832.311.141) ist der Lieferant für die Einhaltung der gesetzlichen Safety-Konformitäten verantwortlich. Darüber hinaus enthält auch die Norm SIA 118 weitere Safety Bestimmungen.

Der Lieferant verpflichtet sich, im Rahmen der ihm übertragenen Aufgaben alle anwendbaren gesetzlichen Vorgaben betreffend Umwelt, Arbeitnehmerschutz sowie Gesundheit und Sicherheit am Arbeitsplatz stets einzuhalten. Der Lieferant hat sicherzustellen, dass seine genehmigten Subunternehmer und Sublieferanten sich ebenfalls an die vorgenannten Vorschriften halten.

3.3 Spezifische Safety-Verpflichtungen des Lieferanten

Der Lieferant ...



- erfüllt die vertraglich übernommenen Verpflichtungen unter Beachtung der relevanten gesetzlichen Bestimmungen¹ sowie allfälliger Safety-Anweisungen von Swisscom. Dazu gehören insbesondere die Informationstafeln im Eingangsbereich der Swisscom-Gebäude
- setzt ein anerkanntes System für das Management von Safety ein und verfügt über dokumentierte Grundsätze und/oder Verfahren, Infrastruktur und Ausrüstung (z.B. geeignete persönliche Schutzausrüstungen) für Safety
- ist dafür verantwortlich, dass seine Mitarbeitenden und beigezogene Mitarbeitende von Subunternehmern (inkl. temporäre Mitarbeitende) die einschlägigen Vorschriften sowie allfällige Anweisungen von Swisscom hinsichtlich Safety kennen, verstehen und einhalten
- bestätigt, dass Arbeiten mit besonderen Gefahren nur durch Mitarbeitende (auch von Subunternehmen) ausgeführt werden, die über die notwendigen Ausbildungen/Weiterbildungen mit entsprechenden Zertifikaten verfügen. Wird eine gefährliche Arbeit von einer Person allein ausgeführt, so muss der Lieferant diese Person überwachen lassen
- gewährleistet, dass beim Einsatz der Mitarbeitenden alle arbeitsrechtlichen Voraussetzungen erfüllt sind und eine gültige Arbeitserlaubnis vorliegt
- gewährleistet, dass die Mitarbeitenden die Safety Unterweisung bestätigt und verstanden haben;
- gewährleistet, dass die Mitarbeitenden alle Swisscom Schulungen absolvieren, die für ihre Aufgabenerfüllung zwingend vorausgesetzt sind
- kontrolliert und überwacht die Einhaltung der entsprechenden Bestimmungen und Vorschriften fortlaufend
- meldet Arbeitsunfälle, einschliesslich Elektronunfälle externer Personen, die innerhalb der Räumlichkeiten oder direkt bei Anlagen von Swisscom vorkommen, umgehend nach allfällig geleisteten Rettungsmassnahmen der Alarmstelle Swisscom (0800 88 00 88)
- verwendet Swisscom-Räumlichkeiten ausschliesslich zur Erledigung der beauftragten Tätigkeiten.

3.4 Weisungs- und Einsichtsbefugnisse von Swisscom

Swisscom als Auftraggeberin ...

- hat anlässlich von Kontrollen hinsichtlich der Safety Weisungsbefugnisse gegenüber den Mitarbeitenden und Vorgesetzten des Lieferanten sowie aller beteiligten Firmen;
- behält sich das Recht vor, bei drohenden Gefährdungen, schweren Berufsunfällen (BU) oder bei Berufskrankheiten Einsicht in die dazu relevante Dokumentation und Nachweise zu nehmen.

4 Fristen

Im vorliegenden Dokument sind Fristen wie folgt definiert:

Begriff	Frist
Sofort	Binnen von 24 Stunden
Unverzüglich	Innerhalb von 2 Werktagen
Kurzfristig	Innerhalb von 3 Werktagen.

¹ Gemäss SE-01354-C2-HD-Safety Gesetzeskompass



5 Kontaktpersonen und Kommunikation

Sämtliche vertragsrelevante Kommunikation zu diesem Vertragsanhang erfolgt in schriftlicher oder elektronischer Form (E-Mail).

5.1 Kontaktpersonen beim Lieferanten

Der Lieferant meldet eine Kontaktperson zum Thema Security der Ansprechperson bei Swisscom. Änderungen der Kontaktperson zum Thema Security sind der Ansprechperson bei Swisscom unverzüglich bekannt zu geben.

5.2 Notfallkontakt Swisscom

Im Falle eines Notfalls ist die Nummer +41 800 880 088 anzurufen. Dort werden weitere Instruktionen gegeben, wie vorzugehen ist.