Anhang ----- zum Vertrag Nr. -----

INFORMATIONSSICHERHEIT / CYBERSECURITY

1 Anwendungsbereich, Ziel und Inhalt

1.1 Dieser Anhang findet Anwendung auf sämtliche Leistungen der Firma, welche im Rahmen des vorliegenden Vertrags durch die Firma erbracht oder geliefert werden. Der Anhang beschreibt die Mindestanforderungen sowie Pflichten der Firma zur Reduktion von Cyberrisiken (nachfolgend sind Informationssicherheitsrisiken gleichbedeutend mitgemeint) und ergänzt die Forderungen der einschlägigen Gesetzgebung, sowie weiterer kunden- und einsatzortspezifischen Anforderungen.

1.2 In diesem Anhang beziehen sich die Begriffe «Sicherheit», «sicher» oder «sicherheitsrelevant» auf den Schutz und die Resilienz gegenüber Informationssicherheits- oder Cyber-Risiken. Der Bereich der funktionalen Sicherheit (Safety) ist nicht Bestandteil dieses Anhangs.

2 Sicherheitsmanagement

2.1 Die Firma unterhält ein nach Art und Umfang für die zu erbringende Leistung geeignetes, dem anerkannten Stand der Technik entsprechendes, unternehmensbezogenes Sicherheitsmanagementsystem zur Reduktion von Cyberrisken (z.B. nach ISO/IEC 27001 oder IEC 62443-2-1).

2.2 Die Firma stellt sicher, dass ihre eigenen Mitarbeitenden sowie die Mitarbeitenden von Sublieferanten, welche an der Entwicklung und Herstellung der Produkte und Komponenten beteiligt sind oder zur Erbringung von Dienstleistungen eingesetzt werden, bezüglich Cyberrisiken sensibilisiert und ausgebildet sind, die einschlägigen Vorschriften kennen und bezüglich ihrer Integrität angemessen überprüft wurden und regelmässig überprüft werden. Sie stellt zudem sicher, dass diese Mitarbeitenden ihre Zugriffsrechte auf Systeme und Daten der SBB ausschliesslich zur Erfüllung ihrer vertraglichen Pflichten nutzen.

2.3 Im Bereich Software- und Produkteentwicklung implementiert die Firma Prozesse zur Reduktion von Cyberrisiken. Diese basieren auf den Prinzipien «security by design» und «privacy by design», falls Personendaten bearbeitet werden. Die Firma orientiert sich an anerkannten Methoden und Standards wie beispielsweise IEC 62443-4-1 oder NIST SP 800-160.

2.4 Für die Offenlegung von Schwachstellen verfügt die Firma über Richtlinien und Prozesse nach anerkannten Methoden und Standards wie beispielsweise ISO/IEC 29147. Die Prozesse und Richtlinien beinhalten insbesondere Definitionen, wie Meldungen zu Schwachstelle gemacht werden können, wie diese bewertet werden und wie Informationen über Schwachstellen der SBB AG mitgeteilt werden.

2.5 Für die Behandlung von Schwachstellen verfügt die Firma über die notwendigen Prozesse und orientiert sich dabei an anerkannten Methoden und Standards (z.B. ISO/IEC 30111).

3 Ansprechpartner für Cybersecurity

3.1 Zur Koordination von Absprachen, zur Überwachung der Einhaltung der Anforderungen in
diesem Anhang und für weiterführende Vereinbarungen, nennen die Parteien einen verantwortlichen Ansprechpartner.

3.2 Die Parteien stellen sicher, dass Änderungen bei den Ansprechpartnern während der Projekt- und Wartungslaufzeit des Produktes der jeweils anderen Partei zeitnah mitgeteilt werden.

3.3 Die Firma kommuniziert einen allgemeinen Kontakt für Fragen bezüglich Cybersecurity, welcher auch nach Ablauf des Vertrags erreicht werden kann.

4 Sicherheitsvorfälle

4.1 Die Firma informiert die SBB AG umgehend bei relevanten Sicherheitsvorfällen (Incidents).

4.2 Die Firma unterstützt die SBB AG bei Cybersecurity-Vorfällen im Zusammenhang mit ihren Produkten und Services.

4.3 Die Firma verpflichtet sich zu einem angemessenen Logging der Systeme und Produkte, um eine Einbindung in ein zentrales Überwachungssystem zu ermöglichen. Werden die Logdaten von der Firma verwaltet, so stellt sie der SBB AG entsprechende Security-Reportings zur Verfügung und gewährleistet eine ausreichende Vorhaltezeit der Logdaten.

4.4 Bei für die SBB AG relevanten Sicherheitsvorfällen werden alle notwendigen Dokumentationen und Daten zur raschen Behebung des Vorfalls zur Verfügung gestellt.

5 Schwachstellen- und Patchmanagement

5.1 Die Firma informiert die SBB AG proaktiv über relevante Schwachstellen.

5.2 Das Produkt oder der Service verfügt über die Möglichkeit, Fehler in der Software (inkl. Firmware und Betriebssystem), welche zu einem Cybersecurity-Risiko führen, zu beheben. Die Software (inkl. Firmware und Betriebssystem) kann dazu in geeigneter Weise aktualisiert werden.

5.3 Die Firma hat einen etablierten Prozess, um Softwareaktualisierungen bereitzustellen. Der Prozess umfasst die notwendigen Massnahmen, um die Authentizität und Integrität der gelieferten Softwareaktualisierungen sicherzustellen.

5.4 Die Firma stellt sicher, dass Softwareaktualisierungen, welche Cybersecurity-Schwachstellen betreffen, zeitnah bereitgestellt oder eingespielt werden.

6 Auslieferung, Dokumentation und Betrieb

6.1 Liefert die Firma Produkte aus, so stellt sie der SBB AG alle notwendigen Unterlagen zur sicheren Integration und dem sicheren Betrieb des Produkts zur Verfügung. Dies umfasst beispielsweise Architekturdokumente, Informationen zu eingesetzten kryptographischen Algorithmen, Schlüsselmaterial, Benutzerkonten und Passwörter. Die Übermittlung der Unterlagen erfolgt auf sicheren Kanälen oder Ablagen.

6.2 Bei der Lieferung von Software und Softwareaktualisierungen stellt die Firma die notwendigen Mittel wie beispielsweise Checksummen zur Überprüfung der Authentizität und Integrität der Lieferung bereit.

6.3 Die für den sicheren Betrieb des Produkts notwendigen Umgebungsbedingungen, Einstellungen und Schritte für die Inbetriebnahme sind in der Dokumentation eindeutig ausgewiesen. Die Dokumentation muss über den gesamten Lebenszyklus des Produkts zu jedem Zeitpunkt nachgeführt sein.

6.4 Wartungszugänge zu Systemen der SBB AG sind immer zu deklarieren und gemeinsam zu vereinbaren. Sofern möglich und wirtschaftlich sinnvoll, sind die Standard-Wartungszugänge der SBB AG zu verwenden.

7 Abnahme

7.1 Sofern nicht im Vertrag oder in den AGB anderweitig geregelt, gelten die nachfolgenden spezifischen Regelungen zur Abnahme.

7.2 Die SBB AG kann für die Abnahme spezifische Sicherheitsprüfungen wie beispielsweise einen Penetration Test durch interne oder externe Experten verlangen.

7.3 Zeigen sich bei der Prüfung lediglich unkritische Schwachstellen, findet die Abnahme mit Abschluss der Prüfung statt. Die Firma behebt umgehend die festgestellten Schwachstellen und gibt deren Behebung der SBB AG bekannt.

7.4 Zeigen sich bei der Sicherheitsprüfungen kritische Schwachstellen, so wird die Abnahme zurückgestellt. Die Firma behebt umgehend die festgestellten Schwachstellen und lädt die SBB AG rechtzeitig zu einer neuen Prüfung ein.

7.5 Die Aufnahme der produktiven Nutzung gilt nicht als Abnahme, ausser sie werde seitens der SBB AG schriftlich bestätigt.

7.6 Trotz Zurückstellung der Abnahme kann der Vertragsgegenstand der SBB AG in gegenseitigem Einverständnis zur Ingebrauchnahme überlassen werden, wobei sämtliche Rechte und Pflichten der Parteien mit Bezug auf die Abnahme und deren Rechtsfolgen weiterbestehen.

8 Gewährleistung

8.1 Bei der Abnahme oder zu einem späteren Zeitpunkt festgestellte Schwachstellen in den von der Firma gelieferten Produkten oder bereitgestellten Services gelten als Mangel im Sinne des Vertrags und es gelten die entsprechend Gewährleistungspflichten.

9 Kontroll- und Auditrecht der SBB

9.1 Sofern nicht im Vertrag oder in den AGB anderweitig geregelt, gelten die nachfolgenden spezifischen Regelungen zum Kontroll- und Auditrecht.

9.2 Die SBB AG ist berechtigt, zu verlangen, dass die Einhaltung der Verpflichtungen der Firma gemäss Ziffer „Sicherheitsmanagement“ sowie die Einhaltung weiterer wesentlicher Verpflichtungen von einer unabhängigen Stelle überprüft wird. Die Prüfung kann durch die SBB AG selbst oder durch ein unabhängiges Revisionsunternehmen im Rahmen eines Audits durchgeführt werden. Jede Partei übernimmt dabei die jeweils bei sich anfallenden oder beauftragten Kosten selbst. Ohne begründeten Anlass kann die SBB AG einen solchen Audit nicht mehr als einmal pro Kalenderjahr verlangen.

9.3 Wird das Audit nicht von der SBB AG selbst durchgeführt, wird der SBB AG im Auditbericht lediglich der exakte Umfang der Prüfung mitgeteilt und ob die Firma ihren vertraglichen Verpflichtungen nachkommt. Liegt eine Verletzung vor, hat die

SBB AG ein umfassendes Einsichtsrecht in die für die Verletzung relevanten Informationen. In diesem Fall darf die SBB ihre Kostenanteile (inkl. ggf. beauftragte Unternehmen) für die Prüfung an die Firma weiterverrechnen.

9.4 Die Firma räumt der SBB AG und entsprechenden Vertragspartnern der SBB AG das Recht ein, die Hard- und Software des Produkts auf Integrität und Sicherheit zu prüfen (Reverse Engineering). Dies stellt keine Verletzung der Intellectual Property Rights (IPR) der Firma dar.

10 Subunternehmen

10.1 Sofern nicht im Vertrag oder in den AGB anderweitig geregelt, gelten die nachfolgenden spezifischen Regelungen zum Beizug von Subunternehmen.

10.2 Soweit die Firma zur Erfüllung ihrer Leistungen inkl. der Bereitstellung von Produkten Dritte hinzuzieht, muss sie deren Lieferanteil in ihr Sicherheitsmanagement vollständig integrieren und dies auf Verlangen der SBB vorzeigen. Sie unterhält ein geeignetes System zur Beurteilung, Auswahl sowie zur regelmässigen Bewertung der Subunternehmen.

10.3 Die Firma verpflichtet nachweislich die ihr beigezogenen Dritten zur Einhaltung der von ihr übernommen Verpflichtungen unter diesem Anhang oder sichert selbst durch eigene Mittel die Cybersecurity der Vor- bzw. Zulieferungen. Die SBB AG kann von der Firma dokumentierte Nachweise verlangen, dass die Firma sich von der Wirksamkeit des Sicherheitsmanagement bei den von ihr beigezogenen Dritten überzeugt hat.