

Besondere Bedingungen für den Einkauf von IT-/ OT-Material oder - Dienstleistungen (BBE-IT/OT) des Energie Service Biel/Bienne (ESB)

1 Zweck und Anwendungsbereich

- 1.1 Die vorliegenden besonderen Bedingungen (BBE-IT/OT) ergänzen die Allgemeinen Einkaufsbedingungen («AEB») und gelten für Verträge oder Bestellungen zwischen dem Energie Service Biel/Bienne («ESB») und dem Lieferanten («Lieferant»), die sich auf Folgendes beziehen:
 - a) Entwicklung, Bereitstellung, Wartung und Unterstützung von Software;
 - b) Cloud-Dienste, Verwaltung der Infrastruktur und damit verbundene Dienstleistungen;
 - c) Bereitstellung und Wartung von Computerausrüstung;
 - d) IT/OT-Beratungsleistungen.
- 1.2 Der Begriff "Lieferant" bezeichnet nachstehend jede Vertragspartei, die an einem Vertrag im Rahmen der IT/OT-Dienstleistungen beteiligt ist.
- 1.3 Vorliegende BBE-IT/OT haben in den spezifisch festgelegten Aspekten Vorrang vor den AVB.

2 Mitarbeiter, die für die Erfüllung des Vertrags abgestellt sind

- 2.1 Der Lieferant stellt sorgfältig ausgewählte, kompetente und geschulte Mitarbeitende zur Verfügung, um die ordnungsgemässe Ausführung der Leistungen zu gewährleisten. Diese Mitarbeitenden müssen zudem ein Bewusstsein für Computerbedrohungen, Social Engineering und die im Vertrag und in diesen besonderen Bedingungen festgelegten technischen und sicherheitsrelevanten Anforderungen haben.
- 2.2 Der Lieferant hält sich an die vom ESB zur Verfügung gestellten Sicherheits- und Cybersicherheitsvorschriften.
- 2.3 Falls es nicht möglich ist, die für die Dienstleistung eingesetzten kompetenten Mitarbeitenden mit gleichwertiger Erfahrung innerhalb von 30 Tagen zu ersetzen, behält sich der ESB das Recht vor, den Vertrag ohne weitere Vorankündigung zu kündigen.
- 2.4 ESB kann jederzeit ohne Begründungspflicht den Austausch eines Mitarbeiters / einer Mitarbeiterin, welche für die Erbringung der Dienstleistung eingesetzt werden sollte, verlangen.

3 Informatik- und Cybersicherheit

- 3.1 Der Lieferant verpflichtet sich, die höchsten Standards der IT/OT-Sicherheit einzuhalten, einschliesslich:
 - a) Verwendung von aktueller Ausrüstung und Software;
 - b) Implementierung eines signaturbasierten Antivirenprogramms mit Verhaltensanalyse;
 - c) Überwachung der Infrastruktur des Lieferanten, um den Missbrauch von Identitäten der dem ESB zugewiesenen Mitarbeiter zu erkennen;
 - d) Verschlüsselung von Daten während der Übertragung und im Ruhezustand;
 - e) strenge Zugangskontrolle, einschliesslich sicherer und namentlich gekennzeichneter Fernzugänge.
- 3.2 Jeder Sicherheitsvorfall, der sich auf die Daten oder Systeme des ESB auswirkt, muss unverzüglich gemeldet werden. Der Lieferant muss kooperieren, um die Auswirkungen zu begrenzen und die Dienste wiederherzustellen.

4 Dokumentation und Ausbildung

- 4.1 Der Lieferant stellt eine vollständige und kopierfähige Dokumentation in elektronischer oder Papierform zur Verfügung, die mindestens Folgendes enthält:
- Eine detaillierte Kartografie der erbrachten Dienstleistungen und ihrer technischen Architektur;
 - Anleitungen zur Installation, Verwaltung und Nutzung;
 - Einzelheiten zu den vorgenommenen Einstellungen, einschliesslich spezifischer Konfigurationen;
 - den Wartungsplan für die Dienste, einschliesslich der Überwachungs- und Interventionsverfahren, die erforderlich sind, um ihren kontinuierlichen Betrieb zu gewährleisten;
 - Übergangsverfahren zur Gewährleistung der Kontinuität der Dienste im Falle einer Kündigung gemäss nachstehender Ziff. 10.
- 4.2 Bei jeder neuen Version oder jedem grösseren Update führt der Lieferant eine Gap-Analyse zwischen den spezifischen Entwicklungen und den nativen Funktionalitäten durch.

5 Wartung und Updates

Wartung

- 5.1 Der Lieferant erbringt die Wartungsleistungen gemäss dem Vertrag. Diese Leistungen umfassen insbesondere: präventive, kurative, korrektive und entwicklungsfähige Wartung.
- 5.2 Der Zweck der präventiven Instandhaltung besteht darin, die Funktionsfähigkeit der Systeme zu gewährleisten, bevor es zu einem Vorfall kommt. Sie umfasst insbesondere
- die proaktive Überwachung der Systeme, um das Risiko eines Ausfalls zu erkennen;
 - die Überprüfung und Optimierung von Konfigurationen zur Risikominimierung;
 - die Durchführung regelmässiger Tests, um die Leistung und Verfügbarkeit der Systeme zu gewährleisten;
 - die Bereitstellung von Software- und Firmware-Updates, die von den Herstellern veröffentlicht werden, um Schwachstellen oder Fehlfunktionen zu verhindern.
- 5.3 Die kurative Instandhaltung dient dazu, gemeldete oder festgestellte Ausfälle oder Fehlfunktionen zu beheben, um den normalen Betrieb des Systems wiederherzustellen. Sie umfasst insbesondere
- die Diagnose von Störungen oder Vorfällen und die Ermittlung ihrer Ursachen;
 - die Reparatur oder den Austausch der defekten Elemente innerhalb der festgelegten Fristen;
 - die Wiederherstellung der Funktionalität durch notwendige Aktualisierungen oder Anpassungen;
 - die Abgabe eines Berichts an den ESB, in dem die durchgeführten Interventionen detailliert beschrieben werden.
- 5.4 Die korrektive Instandhaltung dient der Behebung von Fehlern, die nach der Inbetriebnahme festgestellt oder gemeldet wurden, ohne dass sie notwendigerweise den unmittelbaren Betrieb beeinträchtigen. Sie umfasst insbesondere
- die Korrektur von Anomalien, die vom ESB gemeldet oder vom Lieferanten identifiziert wurden;
 - das Einspielen von Patches, die zur Behebung von Sicherheitslücken erforderlich sind;
 - die Validierung von Patches mit ESB, bevor sie in Produktion gehen
- 5.5 Entwicklungsfähige Wartung dient der Anpassung von Systemen an sich ändernde Bedürfnisse, gesetzliche Anforderungen oder des technologischen Umfelds. Sie umfasst insbesondere
- die Integration neuer Funktionen, die mit dem ESB vereinbart wurden;
 - die Anpassung von Software und Systemen an technische oder regulatorische Veränderungen;
 - die Verbesserung der Leistung, um die operativen Anforderungen des ESB zu erfüllen;
 - die Bereitstellung von grösseren (Upgrades) und kleineren (Updates) Aktualisierungen, die die Kompatibilität mit dem Bestehenden gewährleisten.

Verantwortlichkeiten des Anbieters

- 5.6 Der Lieferant garantiert, dass alle Wartungsleistungen in Übereinstimmung mit den anerkannten Regeln der Technik und den mit dem ESB vereinbarten Spezifikationen durchgeführt werden.
- 5.7 Der Lieferant verpflichtet sich, den ESB über Änderungen an Systemen, Software oder Geräten im Rahmen der Wartung zu informieren.
- 5.8 Für jede Intervention legt der Lieferant einen Bericht vor, der die durchgeführte Intervention, die angewandten Korrekturmassnahmen und etwaige Empfehlungen detailliert beschreibt.

6 Systemüberwachung und Behebung von Schwachstellen

- 6.1 Der ESB behält sich das Recht vor, die vom Lieferanten gelieferten oder unterhaltenen Informationssysteme jederzeit zu überprüfen und / oder zu überwachen, um Anomalien oder Sicherheitsschwachstellen gemäss den vertraglichen Verpflichtungen und den geltenden Standards zu erkennen.
- 6.2 Die bei diesen Überprüfungen festgestellten Abweichungen sind vom Lieferanten innerhalb einer der Schwere der Abweichung angemessenen Frist zu beheben (gemäss dem standardisierten Bewertungssystem CVSS):
 - a) Kritisch: 7 Kalendertage
 - b) Hoch: 14 Kalendertage
 - c) Mittel: 30 Kalendertage
 - d) Niedrig: 60 Kalendertage
- 6.3 Falls eine Schwachstelle nicht innerhalb des festgelegten Zeitrahmens behoben werden kann, kann der Lieferant einen Einsatzplan vorschlagen, der sowohl sofortige und vorübergehende Umgehungsmassnahmen als auch langfristige Behebungsmassnahmen umfasst. Dieser Zeitplan muss vom ESB schriftlich validiert werden. Solange diese Validierung nicht erteilt ist, bleiben die geltenden Fristen in Kraft und die vertraglich vereinbarten Strafen kommen zur Anwendung.

7 Service Level Agreements (SLA)

- 7.1 Der Lieferant garantiert ein Serviceniveau, welches den Anforderungen des ESB gerecht wird und anhand von Indikatoren gemessen wird, die in diesen besonderen Bedingungen festgelegt sind.

Verfügbarkeit von Diensten

- 7.2 Der Lieferant garantiert eine minimale Verfügbarkeit der Dienste von 99% die monatlich auf einer 24/7-Basis berechnet wird, sofern im Vertrag nichts anderes vereinbart ist.
- 7.3 Geplante Ausfallzeiten (planmässige Wartung) müssen dem ESB mindestens 14 Werktage im Voraus mitgeteilt und von ESB genehmigt werden.
- 7.4 Im Falle einer ungeplanten Nichtverfügbarkeit verpflichtet sich der Lieferant, den ESB innerhalb einer Frist von maximal 4 Stunden zu benachrichtigen und unverzüglich Korrekturmassnahmen einzuleiten.
- 7.5 Die Fehlerbehebung erfolgt je nach Art des Vorfalls entweder aus der Ferne oder vor Ort. Im Falle einer Fehlerbehebung aus der Ferne werden die für die Intervention erforderlichen Werkzeuge, einschliesslich solcher, die eine Verbindung und den Austausch von Informationen ermöglichen, vom ESB in Übereinstimmung mit den geltenden Sicherheitsanforderungen festgelegt.

Verwaltung von Vorfällen

7.6 Vorfälle werden nach ihrer Schwere eingestuft:

- a) Kritisch: Ein Vorfall, der sich auf den gesamten Betrieb oder wesentliche Funktionen auswirkt (z.B. Totalausfall von Diensten, kritische Sicherheitslücke).
- b) Mittel: Ein Vorfall, der sich teilweise auf den Betrieb auswirkt (z. B. Systemausfall, Ausfall einer nicht wesentlichen Funktion).
- c) Gering: Ein kleiner Vorfall, der sich nicht auf den laufenden Betrieb auswirkt (z. B. Probleme mit der Benutzeroberfläche oder fehlende Dokumentation).

7.7 Der Lieferant verpflichtet sich, die folgenden Fristen für Vorfälle einzuhalten:

- a) Kritisch: Maximale Antwortzeit: 1 Stunde;
Maximale Lösungszeit: 24 Stunden.
- b) Mittel: Maximale Antwortzeit 2 Stunden;
Maximale Lösungszeit: 2 Tage.
- c) Gering: Maximale Antwortzeit: 4 Stunden;
Maximale Lösungszeit: 3 Tage.

8 Vertraulichkeit und Datenschutz

8.1 Eine Vertraulichkeitsvereinbarung (NDA) für vorvertragliche Beziehungen, sofern eine solche nicht bereits besteht, wird in allen Fällen verlangt, in denen ein Zugang zu Software und/oder Daten erforderlich ist.

8.2 Der Lieferant schützt die Daten des ESB, einschliesslich:

- a) Persönliche Daten und
- b) Technische Daten (Einstellungen, Konfigurationen, Architektur).

8.3 Jede Datenvernichtung am Ende der Vertragslaufzeit muss durch den Lieferanten dokumentiert und vom ESB bestätigt werden.

8.4 Während der in Ziff. 10 definierten Übergangszeit verpflichtet sich der Lieferant, die in diesem Kapitel definierten Geheimhaltungsverpflichtungen für alle übertragenen Informationen einzuhalten.

9 Verantwortung

9.1 Der Lieferant haftet für alle direkten oder indirekten Schäden, die sich ergeben aus:

- a) Fehler in der gelieferten Software, Hardware oder Leistung;
- b) Verzögerungen bei der Anwendung von Sicherheits-Patches oder vereinbarten Updates;
- c) Verstösse gegen die im Vertrag oder in diesen besonderen Bedingungen festgelegten Cybersicherheitsstandards;
- d) Versäumnisse bei der Erfüllung der in Ziff. 10 vorgesehenen Übergangs- oder Transferverpflichtungen.

9.2 Die folgenden Strafen gelten für Verzögerungen bei der Behebung von Schwachstellen:

- a) Kritisch: CHF 1 000.00/Tag
- b) Hoch: CHF 500.00/Tag
- c) Mittel: CHF 250.00/Tag
- d) Gering: CHF 100.00/Tag

10 Umkehrbarkeit

10.1 Im Falle einer Kündigung des Vertrags garantiert der Lieferant eine Übergangszeit von mindestens 3 Monaten, in der er weiterhin die Dienste erbringt, die für die Aufrechterhaltung des ESB-Betriebs erforderlich sind.

- 10.2 Der Lieferant verpflichtet sich, mit dem ESB und/oder jedem anderen vom ESB beauftragten Lieferanten umfassend zu kooperieren, um einen reibungslosen Transfer von Daten, Wissen und Verantwortlichkeiten zu gewährleisten. Diese Zusammenarbeit umfasst insbesondere:
- a) Die Übergabe aller relevanten Dokumentationen, Konfigurationen und Werkzeuge, die für den Betrieb oder die Wartung der betreffenden Dienste erforderlich sind.
 - b) Schulung und Unterstützung des ESB-Personals oder des designierten neuen Lieferanten.
 - c) Die Bereitstellung detaillierter Berichte über den Zustand der Systeme und Leistungen zum Zeitpunkt der Kündigung.
- 10.3 Während der Übergangszeit behält der Lieferant die notwendigen Zugänge zu Daten, Software und Systemen nur im Rahmen der geplanten Operationen bei, um die Kontinuität der Dienstleistungen und die Übertragung der Verantwortlichkeiten zu gewährleisten. Diese Zugriffe müssen strikt auf die notwendigen Operationen beschränkt sein, sicher sein und den Vertraulichkeitsanforderungen gemäss Ziff. 8 entsprechen. Jede Forderung nach zusätzlichen Zahlungen für die Übergangszeit muss im Voraus schriftlich mit dem ESB vereinbart werden.
- 10.4 Die Übergangszeit gilt erst dann als abgeschlossen, wenn der ESB schriftlich bestätigt, dass der Transfer vollständig ist und alle Verpflichtungen des Lieferanten erfüllt wurden.

Im Falle von Widersprüchen zwischen der deutschen und der französischen Fassung ist die französische Fassung massgebend.

Version vom 30.01.2025