

## Conditions particulières d'achat de matériel ou de prestations informatiques d'Energie Service Biel/Bienne (ESB) (CPA IT)

### 1 Objet et champ d'application

- 1.1 Les présentes Conditions Particulières («CPA IT») complètent les Conditions Générales d'Achat («CGA») et s'appliquent aux contrats ou commandes («Contrat») entre Energie Service Biel/Bienne («ESB») et le Fournisseur («Fournisseur»), portant sur:
  - a) Développement, fourniture, maintenance et support de logiciels.
  - b) Services cloud, gestion des infrastructures et services associés.
  - c) Fourniture et maintenance de matériel informatique.
  - d) Prestations de conseil en informatique.
- 1.2 Dans les présentes CPA IT, le terme «Fournisseur» désigne toute partie contractante intervenant dans le cadre d'un Contrat relevant des prestations IT.
- 1.3 Elles prévalent sur les CGA pour les aspects spécifiquement définis.

### 2 Collaborateurs affectés à l'exécution du contrat

- 2.1 Le Fournisseur met à disposition des collaborateurs soigneusement choisis, compétents et formés pour assurer l'exécution des prestations dans les règles de l'art. Ces collaborateurs doivent également être sensibilisés aux menaces informatiques, à l'ingénierie sociale, et aux exigences techniques et de sécurité définies dans le Contrat et les présentes Conditions Particulières.
- 2.2 Le Fournisseur respecte les prescriptions de sécurité et de cybersécurité fourni par ESB.
- 2.3 En cas d'incapacité de remplacement des collaborateurs compétents et d'expérience équivalente affectés à la prestation dans un délai de 30 jours, ESB se réserve le droit de résilier le contrat sans autre préavis.
- 2.4 ESB peut à tout moment demander le remplacement d'un collaborateur affecté à la prestation, sans obligation de justifier cette décision.

### 3 Sécurité informatique et cybersécurité

- 3.1 Le Fournisseur s'engage à respecter les normes de sécurité informatique les plus strictes, notamment:
  - a) Utilisation d'équipements et logiciels à jour
  - b) Mise en œuvre d'un antivirus à base de signature et d'analyse comportementale
  - c) Supervision de l'infrastructure du Fournisseur pour détecter les utilisations frauduleuses des identités des collaborateurs affectés à ESB
  - d) Chiffrement des données en transit et au repos
  - e) Contrôle d'accès strict, incluant des accès distants sécurisés et nominatifs
- 3.2 Tout incident de sécurité affectant les données ou systèmes d'ESB doit être signalé immédiatement. Le Fournisseur doit coopérer pour limiter l'impact et rétablir les services.

### 4 Documentation et formation

- 4.1 Le Fournisseur fournit une documentation complète et copiable, en format électronique ou papier, contenant au minimum:
  - a) Une cartographie détaillée des services fournis et de leur architecture technique ;
  - b) Les guides d'installation, d'administration, et d'utilisation ;
  - c) Les détails des paramétrages réalisés, y compris les configurations spécifiques ;
  - d) Le plan de maintenance des services, incluant les procédures de surveillance et d'intervention nécessaires pour garantir leur fonctionnement continu ;
  - e) Les procédures de transition pour garantir une continuité des services en cas de résiliation, conformément au ch. 10.

- 4.2 Pour toute nouvelle version ou mise à jour majeure, le Fournisseur réalise une analyse d'écart entre les développements spécifiques et les fonctionnalités natives.

## 5 Maintenance et mises à jour

### *Maintenance*

- 5.1 Le Fournisseur assure les prestations de maintenance conformément au Contrat. Ces prestations incluent notamment: la maintenance préventive, curative, correctrice et évolutive.
- 5.2 La maintenance préventive a pour objectif de garantir le bon fonctionnement des systèmes avant qu'un incident ne survienne. Elle inclut et sans s'y limiter:
- La surveillance proactive des systèmes pour identifier les risques de défaillance.
  - La vérification et l'optimisation des configurations pour réduire les risques.
  - La réalisation de tests périodiques pour assurer la performance et la disponibilité des systèmes.
  - Le déploiement des mises à jour logicielles et micrologicielles (firmware) publiées par les fabricants afin de prévenir les vulnérabilités ou dysfonctionnements.
- 5.3 La maintenance curative vise à remédier aux pannes ou dysfonctionnements signalés ou détectés, afin de rétablir le fonctionnement normal du système. Elle inclut et sans s'y limiter:
- Le diagnostic des pannes ou incidents et l'identification de leurs causes.
  - La réparation ou le remplacement des éléments défectueux dans les délais définis.
  - Le rétablissement des fonctionnalités via des mises à jour ou ajustements nécessaires.
  - La remise à ESB d'un rapport détaillant les interventions effectuées.
- 5.4 La maintenance correctrice vise à corriger les anomalies identifiées ou signalées après la mise en service, sans qu'elles affectent nécessairement le fonctionnement immédiat. Elle inclut et sans s'y limiter:
- La correction des anomalies signalées par ESB ou identifiées par le Fournisseur.
  - Le déploiement des correctifs nécessaires pour résoudre les vulnérabilités de sécurité.
  - La validation des correctifs avec ESB avant leur mise en production.
- 5.5 La maintenance évolutive vise à adapter les systèmes aux évolutions des besoins, exigences légales ou des environnements technologiques. Elle inclut et sans s'y limiter:
- L'intégration de nouvelles fonctionnalités convenues avec ESB.
  - L'adaptation des logiciels et systèmes aux changements techniques ou réglementaires.
  - L'amélioration des performances pour répondre aux exigences opérationnelles d'ESB.
  - La fourniture de mises à jour majeures (upgrades) et mineures (updates) garantissant la compatibilité avec l'existant.

### *Responsabilités du Fournisseur*

- 5.6 Le Fournisseur garantit que toutes les prestations de maintenance sont exécutées conformément aux règles de l'art et aux spécifications convenues avec ESB.
- 5.7 Le Fournisseur s'engage à informer ESB des modifications apportées aux systèmes, logiciels ou équipements dans le cadre de la maintenance.
- 5.8 Pour chaque intervention, le Fournisseur fournit un rapport détaillant l'intervention réalisée, les mesures correctives appliquées, et les éventuelles recommandations.

## 6 Supervision des systèmes et correction des vulnérabilités

- 6.1 ESB se réserve le droit de superviser et/ou auditer en tout temps les systèmes d'information fournis ou maintenus par le Fournisseur pour détecter les anomalies ou vulnérabilités de sécurité, conformément aux obligations contractuelles et aux normes applicables.
- 6.2 Les anomalies identifiées lors de ces vérifications doivent être corrigées par le Fournisseur dans des délais proportionnels à leur gravité (selon le système d'évaluation standardisé :CVSS):

- a) Critique: 7 jours calendaires
- b) Élevé: 14 jours calendaires
- c) Moyen: 30 jours calendaires
- d) Faible: 60 jours calendaires

6.3 En cas d'impossibilité de résoudre une vulnérabilité dans les délais définis, le Fournisseur peut proposer un planning de déploiement comprenant des mesures de contournement immédiates et temporaires ainsi que des mesures de remédiation à long terme. Ce planning doit être validé par ESB par écrit. Tant que cette validation n'est pas accordée, les délais applicables restent en vigueur et les pénalités continuent de s'appliquer.

## 7 Service Level Agreements (SLA)

7.1 Le Fournisseur garantit un niveau de service conforme aux besoins d'ESB, mesuré à travers des indicateurs définis dans les présentes Conditions Particulières.

### *Disponibilité des services*

- 7.2 Le Fournisseur garantit une disponibilité minimale de 99% des services, calculée mensuellement sur une base 24/7, sauf stipulation contraire dans le Contrat.
- 7.3 Les périodes d'indisponibilité planifiées (maintenance programmée) doivent être communiquées à ESB au moins 14 jours ouvrés à l'avance et approuvées par ESB.
- 7.4 En cas d'indisponibilité non planifiée, le Fournisseur s'engage à notifier ESB dans un délai maximal de 4 heures et à initier les actions correctives immédiatement.
- 7.5 Le dépannage sera effectué à distance ou sur site, selon la nature de l'incident. En cas de dépannage à distance, les outils nécessaires à l'intervention, y compris, mais sans s'y limiter, à ceux permettant la connexion et l'échange d'informations, seront déterminés par ESB, en conformité avec les exigences de sécurité applicables.

### *Gestion des incidents*

- 7.6 Les incidents sont classés selon leur gravité:
  - a) Critique: Incident impactant l'ensemble des opérations ou les fonctions essentielles (par exemple, interruption totale des services, faille de sécurité critique).
  - b) Moyen: Incident impactant partiellement les opérations (par exemple, un système dégradé, une fonction non essentielle indisponible).
  - c) Faible: Incident mineur n'impactant pas les opérations courantes (par exemple, problème d'interface utilisateur ou documentation manquante).
- 7.7 Le Fournisseur s'engage à respecter les délais suivants pour les incidents:
  - a) Critique: Temps de réponse maximum 1 heure;  
Temps de résolution maximum 24 heures.
  - b) Moyen: Temps de réponse maximum 2 heures;  
Temps de résolution maximum 2 jours ouvrés.
  - c) Faible: Temps de réponse maximum 4 heures;  
Temps de résolution maximum 3 jours ouvrés.

## 8 Confidentialité et protection des données

- 8.1 Un accord de confidentialité (NDA) pour les relations précontractuelles, sauf si un tel accord est déjà en place, est exigé dans tous les cas où un accès à des logiciels et/ou données est nécessaire.
- 8.2 Le Fournisseur protège les données d'ESB, incluant:
  - a) Données personnelles
  - b) Données techniques (paramétrages, configurations, architecture)

- 8.3 Toute destruction de données en fin de contrat doit être documentée par le Fournisseur et validée par ESB.
- 8.4 Pendant la période de transition définie au ch. 10, le Fournisseur s'engage à respecter les obligations de confidentialité définies dans le présent chapitre pour toutes les informations transférées.

## 9 Responsabilité

- 9.1 Le Fournisseur est responsable de tous les dommages directs ou indirects résultant de:
- Défauts de logiciels, matériels ou prestations fournis;
  - Retards dans l'application des correctifs de sécurité ou des mises à jour convenues;
  - Violations des normes de cybersécurité définies dans le Contrat ou les présentes Conditions Particulières;
  - Manquements aux obligations de transition ou de transfert prévues au ch. 10.
- 9.2 Les pénalités suivantes s'appliquent en cas de retard dans la correction des vulnérabilités:
- Critique: CHF 1 000.00/jour
  - Élevé: CHF 500.00/jour
  - Moyen: CHF 250.00/jour
  - Faible: CHF 100.00/jour

## 10 Réversibilité

- 10.1 En cas de résiliation du Contrat, le Fournisseur garantit une période de transition d'une durée minimale de 3 mois, pendant laquelle il continue à fournir les services nécessaires pour assurer la continuité des opérations d'ESB.
- 10.2 Le Fournisseur s'engage à coopérer pleinement avec ESB et/ou tout autre fournisseur désigné par ESB, afin de garantir un transfert fluide des données, des connaissances, et des responsabilités. Cette coopération inclut et sans s'y limiter:
- La remise de toutes les documentations pertinentes, configurations, et outils nécessaires au fonctionnement ou à la maintenance des services concernés.
  - La formation et l'assistance au personnel d'ESB ou au nouveau fournisseur désigné.
  - La mise à disposition de rapports détaillés sur l'état des systèmes et prestations à la date de résiliation.
- 10.3 Pendant la période de transition, le Fournisseur maintient les accès nécessaires aux données, logiciels, et systèmes uniquement dans le cadre des opérations prévues pour assurer la continuité des services et le transfert des responsabilités. Ces accès doivent être strictement limités aux opérations nécessaires, sécurisés, et conformes aux exigences de confidentialité définies au ch. 8. Toute demande de paiement supplémentaire pour la période de transition doit être convenue par écrit au préalable avec ESB.
- 10.4 La période de transition est considérée comme achevée uniquement lorsque ESB confirme par écrit que le transfert est complet et que toutes les obligations du Fournisseur ont été remplies.

*En cas de contradiction entre la version allemande et la version française, la version française fait foi.*

*Version du 17.01.2025*