Conditions générales du canton de Berne
relatives à la sûreté de l'information et à la protection des données (SIPD)
dans la fourniture de services informatiques V3.0
(CG SIPD)

1. Dispositions générales

1.1 But

Les présentes conditions générales (CG) ont pour but de protéger les droits de la personnalité des personnes dont les données sont traitées et de garantir la sûreté de l'information lorsque des tiers fournissent des services informatiques au canton de Berne.

1.2 Notions

a) *Fournisseurs de prestations :* personnes physiques et morales, ainsi qu'institutions de droit public, qui fournissent des services informatiques au canton de Berne.

b) *Bénéficiaire de prestations :* le canton de Berne, représenté par ses organes ou services, comme le Conseil-exécutif, les Directions, la Chancellerie d'Etat, les unités administratives, les offices, les entreprises et les tribunaux qui confient aux fournisseurs de prestations la fourniture de services informatiques.

c) *Services informatiques :* prestations dans le domaine de l'informatique et des télécommunications, en particulier les services de communication et de centres de calcul, la mise sur pied et l'exploitation de systèmes de bureautique ainsi que la conception et la maintenance d'applications.

1.3 Objet et champ d'application

[1] Les présentes conditions générales s'appliquent aux services informatiques fournis au bénéficiaire par le fournisseur de prestations qui comportent le traitement de données du bénéficiaire ainsi qu'aux processus administratifs du fournisseur de prestations qui sont en rapport avec ces services.

[2] Les présentes conditions générales s'appliquent aussi aux sous-traitants et sous-traitantes, aux mandataires, aux auxiliaires et aux collaborateurs et collaboratrices du fournisseur de prestations qui s'occupent de données, de systèmes et de processus du bénéficiaire de prestations.

1.4 Rapport avec les dispositions contractuelles

[1] Les présentes conditions générales font partie intégrante d'un contrat conclu entre le fournisseur et le bénéficiaire des prestations. Si ce contrat prévoit que d'autres CG feront foi, notamment les « CG TIC-Services de la Conférence suisse sur l'informatique » (CG CSI), les dispositions des présentes conditions générales se substituent aux dispositions des autres CG en matière de sûreté de l'information et de protection des données.

[2] Au surplus, les dispositions des autres éléments contractuels priment sur les présentes conditions générales.

2. Droits et obligations des parties

2.1 Obligation d'information

[1] Le fournisseur de prestations informe le bénéficiaire de manière documentée, à la demande de celui-ci, sur les méthodes et processus qu'il utilise pour fournir ses services contractuels et qui revêtent une importance en vue du respect des directives SIPD. Le bénéficiaire des prestations peut consulter les documents ad hoc sur place et demander une démonstration des processus administratifs.

[2] Le fournisseur de prestations avertit immédiatement le bénéficiaire de tout incident exceptionnel qui concerne les données, les systèmes et les processus de celui-ci, en particulier des violations importantes des directives SIPD.

2.2 Respect de la protection de base SIPD

Le fournisseur de prestations garantit la protection de base SIPD conformément à l'annexe 1 des présentes conditions générales. Le contrat précise les particularités de la protection de base SIPD applicables au cas d'espèce.

2.3 Respect de consignes SIPD supplémentaires selon concept SIPD

Si les exigences SIPD du bénéficiaire de prestations dépassent le niveau de la protection de base SIPD, le contrat contient un concept SIPD qui régit les exigences et les mesures ad hoc.

2.4 Obligations découlant de la loi sur la protection des données

Le fournisseur de prestations prend acte de la teneur de l'article 16 de la loi cantonale du 19 février 1986 sur la protection des données (LCPD, RSB 152.04) :
« *Celui qui traite des données personnelles sur mandat d'une autorité a, vis-à-vis de la loi, la même position que son mandant. Il ne communiquera de données personnelles à des tiers que si le mandant y donne son accord exprès.* »[1]

2.5 Sous-traitance

[1] Le contrat ou les autres CG applicables déterminent si, et dans quelle mesure, le fournisseur de prestations peut avoir recours à des tiers. Ceux-ci doivent toutefois s'engager par écrit à respecter l'obligation de conserver le secret au sens de l'alinéa 2 qui est une condition impérative de la sous-traitance.

[2] Le fournisseur de prestations impose aux tiers auxquels il a recours (ch. 1.3, al. 2 des présentes CG) l'obligation de s'engager par écrit à respecter l'obligation de conserver le secret (ch. 2.6) et prescrit le respect des dispositions légales et contrac-

[1] La version actuelle de cette loi est accessible sur le site internet du Recueil systématique bernois RSB (www.sta.be.ch/belex).

tuelles en matière de SIPD dans le contrat de travail qu'il conclut avec le personnel prêté au bénéficiaire des prestations. Il informe les tiers concernés des dispositions légales et contractuelles en matière de SIPD.

2.6 Obligation de garder le secret

[1] Le fournisseur de prestations doit garder le secret sur les faits et données qui ne sont ni notoires ni généralement accessibles. En cas de doute, les faits et données doivent être traités de manière confidentielle. L'obligation de garder le secret naît dès avant la conclusion du contrat et persiste au-delà de la fin des rapports contractuels ou de la fourniture de la prestation convenue. Les devoirs légaux de renseigner sont réservés.

[2] Le fournisseur de prestations a le droit de communiquer le fait et la teneur essentielle de la demande d'offre aux tiers à qui il confiera éventuellement des mandats. La publicité portant sur des prestations du projet et la publication de celles-ci requièrent le consentement écrit du bénéficiaire des prestations.

2.7 Transmission de données et d'informations

[1] Sauf autorisation contraire, le fournisseur de prestations ne peut utiliser les données du bénéficiaire qu'au bénéfice de celui-ci et ne peut les communiquer qu'à celui-ci. Les requêtes de divulgation de données présentées par des personnes privées (concernées ou non par le traitement de ces données), par d'autres autorités ou par d'autres services de l'administration cantonale doivent être transmises au bénéficiaire des prestations.

[2] Les mesures de contrainte prévues par les codes de procédure et ordonnées par les autorités compétentes sont réservées. Dans ces cas aussi, le fournisseur des prestations doit informer immédiatement le bénéficiaire ou lui adresser le requérant ou la requérante, dans la mesure où la loi le lui permet.

2.8 Audits SIPD

[1] Le bénéficiaire des prestations peut ordonner des audits SIPD auprès du fournisseur, portant sur ses données, systèmes et processus. Les audits sont réalisés par des services internes ou externes, compétents et indépendants au plan technique, selon des méthodes reconnues. Le fournisseur de prestations n'est pas tenu de collaborer avec des auditeurs avec lesquels il se trouve en situation de concurrence. Le bénéficiaire des prestations fait parvenir le rapport d'audit au fournisseur des prestations.

[2] Si le fournisseur de prestations est certifié conforme à des normes reconnues en matière de sûreté de l'information et de protection des données, et passe de ce fait régulièrement des audits, il fait parvenir le rapport d'audit au bénéficiaire des prestations lorsque ce rapport concerne les données, systèmes et processus de celui-ci.

[3] Le contrat règle les détails, le cas échéant.

2.9 Surveillance et contrôle

[1] Dans la mesure où des données, systèmes et processus du bénéficiaire des prestations sont concernés, le fournisseur de prestations est soumis à la surveillance de

l’autorité cantonale de surveillance (art. 32 ss LCPD) en matière de protection des données, secondée par le délégué ou la déléguée à la sûreté de l’information (DSI BE) de l’Office cantonal d’informatique et d’organisation.

[2] Dans l’accomplissement de ses tâches légales, l’autorité de surveillance peut réaliser ou faire réaliser des contrôles. A cet effet, le fournisseur de prestations la seconde à titre gracieux.

2.10 Assistance du bénéficiaire de prestations

Le bénéficiaire des prestations aide le fournisseur à s’acquitter de ses obligations selon les dispositions des présentes conditions générales.

3. Sanctions

La violation des chiffres 2.5, alinéas 2, 2.6 et 2.7 des présentes conditions générales est sanctionnée par les dispositions chiffres 13.4 des CG CSI .

4. For et droit applicable

Si aucun autre document contractuel ne régit le for ou le droit applicable, le for est Berne et les présentes conditions générales sont soumises au droit suisse.

Annexe 1 : Protection de base SIPD

En vertu de l'Ordonnance de Direction du 3 janvier 2011 concernant la sûreté de l'information et la protection des données (OD SIPD, RSB 152.040.2), les mesures de protection de base SIPD doivent être mises en œuvre pour tous les traitements de données dans l'administration cantonale.

Nous reproduisons ci-dessous les dispositions du module Protection de base du Guide SIPD de l'Office d'informatique et d'organisation qui relèvent des fournisseurs de prestations. Le contrat précise les particularités applicables au cas d'espèce (ch. 2.2 des CG SIPD).

1. Contrôle des accès (physique)
Objectif : empêcher l'accès aux locaux où des données personnelles sont traitées.

1.1 Mesures d'ordre organisationnel

1.1.1 Affecter les locaux sensibles (où se trouvent p.ex. le serveur, d'importants équipements de télécommunication, des copies de sécurité, des archives) aux zones de sécurité.

1.1.2 Régir l'accès aux locaux et aux outils informatiques par des autorisations d'accès compréhensibles et contraignantes, logiquement hiérarchisées.

1.1.3 Elaborer et documenter un plan de fermeture régissant les responsabilités, la gestion, l'attribution et le retrait des moyens d'accès.

1.2 Mesures d'ordre technique

1.2.1 Equiper les entrées des zones de sécurité d'un système d'accès et de verrouillage sûr.

1.2.2 Contrôler régulièrement le bon fonctionnement des systèmes d'accès et de verrouillage.

1.2.3 Empêcher l'entrée par d'autres ouvertures du bâtiment grâce à l'installation de grilles aux fenêtres, de stores de sécurité, etc.

2. Contrôle des accès
Objectif : empêcher que des personnes non autorisées utilisent des installations, services ou applications informatiques et des équipements de communication, ou qu'elles consultent des données du bénéficiaire des prestations.

2.1 Mesures d'ordre organisationnel

2.1.1 Régir, documenter et surveiller de manière contraignante l'attribution de comptes utilisateur.

2.1.2 Bloquer ou supprimer les comptes et les droits d'accès qui ne sont plus nécessaires (p.ex. en cas de départ) ou qui n'ont plus été utilisés depuis longtemps.

2.1.3 Veiller, aux alentours des guichets, secrétariats et autres secteurs ouverts au public, à empêcher que des appareils périphériques puissent être consultés par des personnes non autorisées.

2.2 Mesures d'ordre technique

2.2.1 Soumettre l'autorisation d'accès aux systèmes à une identification de l'utilisateur et à un mot de passe sûr. Les mots de passe doivent satisfaire aux exigences suivantes :

- Les mots de passe sont personnels et confidentiels.
- Ils se composent d'au moins 8 caractères et doivent combiner des lettres et des caractères spéciaux ou des chiffres.
- Le mot de passe ne peut pas être identique au nom d'utilisateur.
- La validité est limitée à 30 jours ou à 3 tentatives infructueuses.

2.2.2 Bloquer l'accès après 3 tentatives d'identification infructueuses.

2.2.3 Enregistrer les tentatives d'identification infructueuses dans un journal et passer régulièrement les journaux en revue.

2.2.4 Garantir que seuls des utilisateurs habilités puissent avoir accès aux appareils périphériques (p.ex. imprimantes) et les commander.

3. Contrôle des accès (logique)
Objectif : empêcher que des personnes habilitées à utiliser le système n'accèdent à des données sans y être autorisées

3.1 Mesures d'ordre organisationnel

3.1.1 Elaborer et instaurer un concept des droits d'utilisateur approprié et contraignant, fondé sur des rôles d'utilisateur définis selon le principe de "qui a besoin de savoir quoi" au niveau des applications.

3.2 Mesures d'ordre technique

3.2.1 Identifier et authentifier les utilisateurs dans le système à l'aide d'un ID utilisateur et d'un mot de passe sûr (voir ch. 2 ci-dessus).

4. Contrôle des transmissions
Objectif : empêcher toute perte de confidentialité, de disponibilité et d'intégrité pendant la transmission des données

4.1 Mesures d'ordre organisationnel

4.1.1 Edicter des instructions régissant l'utilisation des moyens de transfert de données (fax, internet, téléphone portable, etc.).

4.1.2 Désigner comme tels et identifier clairement les supports de données (papier, disquette, CD, etc.) contenant des données classifiées.

4.1.3 Emballer et adresser de manière adéquate les supports contenant des données personnelles.

4.1.4 Préciser quels utilisateurs et quels opérateurs ont le droit de recourir à quels services de réseau, et contrôler cette utilisation.

4.2 Mesures d'ordre technique

4.2.1 Protéger la confidentialité et l'intégrité des données d'authentification, clés ou autres données système sensibles lors du transfert de données via un réseau.

4.2.2 Enregistrer dans un journal les transferts à partir de/vers des réseaux tiers (établissement de la communication, utilisateurs)..

5. Contrôle des entrées
Objectif : conserver les preuves relatives aux activités des utilisateurs.

5.1 Mesures d'ordre organisationnel

5.1 Réglementer de manière contraignante qui peut traiter quelles données et qui est responsable de la protection et de la qualité des données.

5.2 Mesures d'ordre technique

Aucune.

6. Contrôle des mandats
Objectif: garantir que le traitement des données est conforme au mandat.

6.1 Mesures d'ordre organisationnel

(Ne sont pas pertinentes dans le cadre des présentes conditions générales.)

6.2 Mesures d'ordre technique

6.2.1 Limiter les droits d'accès des partenaires d'externalisation à des applications et des données clairement définies, selon les tâches qui leur sont confiées..

6.2.2 Protéger l'accès extérieur via le réseau par des procédures d'authentification rigoureuses.

7. Contrôle de la disponibilité

Objectif : protéger les données contre l'indisponibilité, la destruction et la perte.

7.1 Mesures d'ordre organisationnel

7.1.1 Consigner sous forme sécurisée les données d'authentification du responsable du système ou d'autres opérateurs système privilégiés pour des suppléances en cas d'urgence.

7.1.2 Veiller, pour la sécurité de l'exploitation, de l'utilisation et de la maintenance des systèmes et des applications, à ce que les documents nécessaires soient en permanence disponibles auprès des responsables de système et d'application.

7.2 Mesures d'ordre technique

7.2.1 Protéger de manière adéquate les locaux et systèmes informatiques (serveur et importantes infrastructures de réseau) contre les dommages physiques (effraction, incendie, inondation, etc.).

7.2.2 Protéger les systèmes par un dispositif contre les surtensions, une alimentation non interruptible et un système de climatisation adéquat.

7.2.3 Contrôler régulièrement les supports choisis pour sécuriser les données (sauvegarde/restauration)..

7.2.4 Conserver les supports de données mobiles et les données correspondantes dans des locaux protégés et séparés physiquement de l'environnement d'exploitation..

8. Contrôle de la séparation

Objectif : garantir le respect du principe d'affectation à des fins déterminées (art. 5, al. 4 LCPD)

8.1 Mesures d'ordre organisationnel

(Ne sont pas pertinentes dans le cadre des présentes conditions générales.)

8.2 Mesures d'ordre technique

8.2.2 Traiter séparément les données de test et les données de production. Une séparation logique fiable est suffisante.

(Les autres mesures ne sont pas pertinentes dans le cadre des présentes conditions générales.)

9. Autres objectifs de contrôle

Objectif : garantir de manière générale la sûreté de l'information.

9.1 Mesures d'ordre organisationnel

9.1.3 Prendre des mesures adéquates en prévision d'un accident majeur, d'une catastrophe ou d'une autre situation d'urgence.

(Les autres mesures ne sont pas pertinentes dans le cadre des présentes conditions générales.)

9.2 Mesures d'ordre technique

9.2.1 Protéger les systèmes et les applications contre les logiciels malveillants à l'aide de produits reconnus (logiciels antivirus).

(Les autres mesures ne sont pas pertinentes dans le cadre des présentes conditions générales.)

* * *