canton de vaud
LIBERTÉ ET PATRIE

Direction générale du numérique et
des systèmes d'information

Avenue de Longemalle 1
CH-1020 Renens

ACCORD DE CONFIDENTIALITÉ DE PERSONNE

Accord de confidentialité et charte de protection des données pour personne interne ou externe

OBJET

Cet accord de confidentialité précise les points sur lesquels les personnes effectuant des travaux pour le compte de la Direction générale du numérique et des systèmes d'information de l'Administration cantonale s'engagent en matière de sécurité de l'information et de protection des données.

Les prescriptions contenues dans ce document s'ajoutent à celles déjà applicables en ce domaine, notamment celles découlant des législations fédérales et cantonales, soit le droit pénal et civil et en particulier les articles. CO 97 et suivants, CPS 143, 143bis, 144, 144bis, 147 et 179^{novies}, les lois sur la protection des données personnelles (LPrD, LPD), ainsi que la loi sur le personnel de l'Etat de Vaud (LPers).

Cet accord de confidentialité est motivé par le fait qu'une personne peut, dans l'exercice de ses fonctions, avoir accès à des données ou à des informations de l'Etat dont le caractère est confidentiel.

CONFIDENTIALITÉ

L'Etat insiste sur l'importance de la confidentialité. Il revient au responsable de traitement de définir la classification des informations traitées. Les informations pouvant être divulguées sont publiques ou autorisées par une autorité, une fonction ou une loi.

PROTECTION DES DONNÉES

La protection de la vie privée et des données personnelles est un sujet sensible. C'est la raison pour laquelle la législation prévoit que leur traitement ne peut se faire que si une base légale l'autorise ou s'il sert à l'accomplissement d'une tâche publique ou qu'un consentement l'autorise. Des exigences sécuritaires renforcées sont exigées pour le traitement de données sensibles (opinions, sphère intime, procédures judiciaires, etc.) ou de profils de la personnalité.

PRESCRIPTIONS

Toute personne qui conçoit, installe, utilise ou supporte des ressources de l'Etat de Vaud prend l'engagement de :

1. Annoncer dans des plus brefs délais, à l'entité de sécurité de la DGNSI ou au Service-Desk, toute tentative de violation, les failles de sécurité ou vulnérabilités identifiées, la perte ou le vol de données ou de matériel de l'ACV, ainsi que tout comportement litigieux ou suspect.
2. Se conformer à la Directive LPers 50.1 sur l'utilisation d'Internet, de la messagerie électronique, de la téléphonie et du poste de travail (aussi pour les externes). Un complément, en préparation, précisera l'usage acceptable de moyens informatiques de l'Etat.
3. Contribuer activement à la sécurité de l'information et à la protection des données et des autres actifs de l'Etat contre tout accès, utilisation, modification, divulgation ou destruction non autorisés. Pour rappel, les actions effectuées sur les systèmes de l'ACV **sont journalisées et surveillées**.
4. Ne jamais divulguer à des tiers ou à des collègues non autorisés des faits ou des informations obtenus dans le cadre de sa mission. Ceci, tant en interne qu'en dehors de l'Etat.
5. Conserver de manière confidentielle et personnelle les mots de passe et toutes données sensibles dont elle serait bénéficiaire et responsable dans le cadre de son mandat.

6. Respecter au mieux les principes de « bureau vide ». Les documents notes, supports de données, etc. ne doivent pas être visibles et, si possible, sous clef hors des heures de travail.
7. En cas d'absence de sa place de travail, verrouiller systématiquement son ordinateur.
8. Ne pas réaliser de photo, d'enregistrement ou de copie non autorisée de données, sous quelque forme que ce soit, même à des fins de tests.
9. S'assurer de l'origine et vérifier la sécurité de tout support de données avant d'en exploiter le contenu. Le chiffrer, dans la mesure du possible.
10. Le matériel homologué par la DGNSI peut être connecté sans autre au système d'information cantonal.
11. L'utilisation de périphériques (entrée, sortie, stockage) dont l'origine et la sécurité sont vérifiées est autorisée pour réaliser sa mission et sans exposer le réseau cantonal (ex : beamer, écran, clavier, souris, matériel de vidéoconférence, smartphone, tablette).
12. Tous les autres périphériques de communication et le matériel réseau doivent être homologués par la DGNSI pour être utilisés sur le réseau cantonal.
13. Restituer et détruire toutes les données, sous quelque format que soit (y compris papier) utilisées en tant que réflexions, jeux de données spécifiques pour corriger un bug, etc. lorsque la conservation n'est plus nécessaire ou que le projet est terminé.
14. Respecter le matériel protégé par les droits d'auteur et le droit à l'image.
15. Garder le secret même après la fin des travaux et tant que l'exige la sauvegarde des intérêts légitimes de l'Etat de Vaud.
16. De par leur nature liée à la sécurité, surveillance ou investigation, certains traitements de données excluent l'anonymisation et l'autorisation formelle du responsable. Ces traitements sont documentés et autorisés par l'entité de sécurité de la DGNSI. Les responsables de traitements sont globalement informés des moyens sécuritaires mis en œuvre.
17. **Dans le cas de prestations de développement**
    a. Se conformer aux exigences spécifiques de la DGNSI et n'utiliser que les logiciels autorisés.
    b. Anonymiser les données sensibles ou confidentielles. Dans le cas où cela n'est pas raisonnablement possible, le responsable de traitement, propriétaire des données, doit limiter l'accès aux données strictement nécessaires à l'exécution du travail concerné.
    c. Ne jamais stocker, de manière non chiffrée, des fichiers contenant des données sensibles ou confidentielles hors des systèmes étatiques.
18. **Dans le cas d'une prestation externalisée**

    S'assurer que les données et informations accédées bénéficient au minimum du même niveau de sécurité physique et logique que dans l'environnement de l'Etat (cf. bonnes pratiques de sécurité de l'information, norme ISO27001).
19. **Depuis l'étranger**
    a. Depuis l'étranger, seules les données professionnelles de la messagerie (e-mail, contacts, agenda) peuvent être accédées en ligne et synchronisées sur du matériel privé.
    b. Tout accès à d'autres données professionnelles non publiques est proscrit hors des frontières suisses.
    c. Dans le cas d'accès depuis l'étranger, avoir obtenu une autorisation formelle de la part de l'entité de sécurité de la DGNSI.
    d. Ne pas franchir les frontières suisses avec un ordinateur de l'Etat, autre que smartphone ou tablette, sans une autorisation formelle de la part de l'entité de sécurité de la DGNSI.

20. **Dans les locaux de la DGNSI**

    a. Un visiteur s'annonce, porte un badge et est systématiquement accompagné d'un collaborateur de la DGNSI.

    b. Restituer son badge et son matériel à la fin de la relation contractuelle.

21. **Les exceptions**

    Chaque prescription peut faire l'objet d'une exception si l'exécution de la mission professionnelle le nécessite. Dans ce cas, des mesures compensatoires sont prises pour limiter le risque. Une exception est documentée et fait l'objet d'une autorisation formelle de l'entité de sécurité DGNSI.

RESPONSABILITES ET SANCTIONS

Le signataire est responsable tant de ses actions que de ses inactions préjudiciables à la sécurité.

Chacun est tenu d'exercer ses droits et d'exécuter ses obligations selon les règles de la bonne foi. L'abus manifeste d'un droit n'est pas protégé.

Le non-respect de ces prescriptions peut entraîner l'application du dispositif prévu par la loi sur le personnel de l'Etat, soit un avertissement avec menace de licenciement, voire un renvoi immédiat en cas de juste motif. Une personne externe risque d'entrainer une rupture de la relation contractuelle et un dédommagement pour le tort causé.

L'accès aux ressources informatiques de l'Etat est subordonné à la signature du présent document.

ACCEPTATION

Par sa signature, la personne concernée certifie qu'elle est employée par l'entité mentionnée ci-après, qu'elle a pris connaissance des dispositions législatives et réglementaires exposées ci-dessus et s'engage à les respecter dans le cadre des travaux exécutés pour le compte de l'Etat. Le secret est maintenu une fois la relation terminée. Le signataire confirme qu'il prendra également connaissance de la politique de sécurité des systèmes d'information de la DGNSI.

Employeur .....

Nom ..... Prénom .....

Adresse ..... Téléphone .....

NPA/localité ..... E-mail .....

Date ..... Lieu .....

Signature .....

Répondant ACV *Service / entité / nom* .....

Objet / projet .....

Original à classer dans le dossier des ressources humaines ou, pour les fournisseurs, avec le premier contrat. Copie remise à l'entité Achats et Contrats de la DGNSI (achats-contrats@vd.ch).