Règles de Sécurité des Systèmes d'Information pour les Prestataires de Services (RSSIPS) à la CDC

Caisse des Dépôts
GROUPE

Interne

Sommaire

01. Introduction 3

02. Accès aux ressources 7

03. Bon usage des ressources 9

04. Propriété intellectuelle 16

05. Protection de l'information et des données à caractère personnel 18

06. Contrôle de l'usage des ressources 20

07. Serveurs de fichiers 22

08. Mention d'information : données à caractère personnel 24

01

Introduction

1.1 Objet du document

- Ce document nommé ci-après les « RSSIPS » (Règles de Sécurité des Systèmes d'informations pour les Prestataires de Services) a pour objectif d'expliquer les règles en vigueur au sein de la CDC et est destiné aux prestataires de services, utilisateurs, même occasionnels, des ressources informatiques de la CDC mises à leur disposition pour les stricts besoins de l'accomplissement de leurs prestations.

- Ces RSSIPS illustrent le comportement respectueux et responsable que chacun s'oblige à adopter vis-à-vis des ressources qui lui sont mises à disposition.

- En conséquence, le prestataire de services, avant toute utilisation des ressources informatiques de la CDC :

    - s'engage à appliquer les présentes RSSIPS dans le cadre de la réalisation des prestations qui lui sont confiées ;
    - se porte fort du respect par tous ses salariés et tous ses éventuels sous-traitants amenés à intervenir dans le cadre de la réalisation des prestations qui lui sont confiées ;
    - s'engage à conserver et à fournir à première demande de la CDC l'attestation originale et signée par ses salariés et ses éventuels sous-traitants amenés à intervenir dans le cadre de la réalisation des prestations qui lui sont confiées, selon le modèle joint en annexe des présentes RSSIPS.

1.2 Définitions

- Par « ressources », on entend tout élément intervenant dans la mise en œuvre et le fonctionnement d'un système d'information (informations sous toutes leurs formes, équipements individuels, imprimante, logiciel, serveur de fichiers, base de données, applicatif, équipement réseau, service réseau interne/externe, espace disque, messagerie électronique, etc…).

- Par « utilisateur », on entend toute personne physique qui accède aux et/ou utilise les ressources de la CDC et de ses clients comprenant le personnel des prestataires de services de la CDC et leurs éventuels sous-traitants.

1.3 Cadre réglementaire

- Les ressources mises à disposition par la CDC et toutes les données qu'elles contiennent sont la propriété de la CDC et/ou de ses clients.

- Il est nécessaire que tout utilisateur de ces ressources, dont les personnels des prestataires (sous-traitants inclus), respectent les politiques générales de sécurité et de confidentialité mises en place par la CDC ainsi que les règles de bonne conduite, formalisées dans le présent document, en conformité avec la législation et la réglementation en vigueur.

- Chaque utilisateur autorisé par la CDC à accéder aux SI de la CDC et/ou de ses clients reste, dans l'usage des ressources, soumis aux lois civiles et pénales générales. Il est seul responsable de toute utilisation des ressources faites à partir de son compte et de ses habilitations et s'engage à ne pas les utiliser dans le cadre d'activités illicites et/ou contraires à l'ordre public et aux bonnes mœurs, et/ou susceptibles de porter préjudice à la CDC, à ses clients et à des tiers mais à les utiliser uniquement dans le cadre de l'exécution des prestations.

- Chaque prestataire de service de la CDC s'engage à faire accepter expressément les règles posées par les présentes RSSIPS à son personnel ainsi qu'à ses éventuels sous-traitants qui seront amenés à utiliser les ressources de la CDC et/ou de ses clients, pour les besoins de l'accomplissement des prestations.

02

Accès aux ressources

Confidentiel

- L'accès par un utilisateur aux ressources de la CDC et/ou de ses clients n'est possible que pour les besoins de l'exécution des prestations, définies dans le contrat de prestations de services, et dans les limites des habilitations qui lui sont accordées, lesquelles peuvent être modifiées ou supprimées par la CDC.

- Les accès aux ressources sont soumis à authentification (un identifiant unique couplé à un authentifiant unique qui peut être un mot de passe) et associés à des habilitations qui doivent être limitées. Accéder à une ressource est une responsabilité personnelle identifiée, avec des droits et des devoirs pour la bonne maîtrise des accès logiques au SI de la CDC.

- Les moyens d'authentification sont personnels, confidentiels et non transmissibles. En conséquence, les utilisations faites à l'aide d'un moyen d'authentification propre à chaque utilisateur sont réputées être le fait du détenteur de ce moyen d'authentification, sauf preuve contraire.

- *L'utilisateur ne doit pas contourner les dispositifs de sécurité d'accès en place ou d'accéder, ou tenter d'accéder à des ressources pour lesquelles il n'est pas habilité.*

03

Bon usage des ressources

Confidentiel

3.1 Bon usage général des ressources

- L'utilisateur est responsable des usages qu'il fait des ressources mises à sa disposition pour les besoins de l'exécution de ses prestations. Ce principe de responsabilité implique des comportements adaptés.

- L'utilisateur ne doit pas, en particulier :
  - Mettre à disposition de personnes non autorisées, que ce soient des personnes internes ou externes à la CDC, les ressources de la CDC et/ou de ses clients ;
  - Tenter de lire, modifier, copier ou détruire des informations autres que celles qui lui appartiennent en propre ou pour lesquelles il dispose des droits correspondants ;
  - Contourner les restrictions d'utilisation des ressources mises à sa disposition par la CDC ;
  - Contourner notamment les dispositifs de lutte contre la fuite de données – *Data Leaks Prevention* (DLP) ou tout dispositif de contrôle ou de surveillance mis en place par la CDC aux fins d'assurer la sécurité de ses systèmes d'information et dont l'utilisateur a été valablement informé ;
  - Copier et traiter des informations et/ou données de la CDC et/ou de ses clients sur un équipement individuel, non propriété de la CDC et sans son autorisation expresse et préalable ;Accéder, s'introduire, se maintenir frauduleusement dans le SI de la CDC et/ou de ses clients et/ou altérer des éléments qu'il contient et/ou empêcher son fonctionnement ainsi qu'effectuer toute tentative à cette fin.

- Seront notamment considérés comme abusifs au sens des RSSIPS, les comportements visant à organiser la réception, consulter ou tenter de consulter, télécharger, conserver, publier, diffuser ou distribuer, en toute connaissance de cause au moyen des ressources de la CDC, tous programmes, logiciels, documents électroniques, messages, Informations, données :

  - Visant à dénigrer la CDC et/ou ses clients, portant atteinte à son image de marque, à ses intérêts ou à sa réputation ;
  - A caractère violent, pédopornographique, pornographique, xénophobe, révisionniste, négationniste, raciste ou sectaire et, plus généralement, contraire à la réglementation en vigueur ;
  - Susceptibles de porter atteinte au respect de la personne humaine, de sa dignité ou de sa vie privée ;

- A caractère diffamatoire ;
- Ayant pour objet le harcèlement, la menace ou l'injure ;
- Contenant des éléments protégés par les lois sur la propriété intellectuelle et le droit à l'image, sauf à posséder les autorisations nécessaires ;
- Incitant à la commission d'un délit ou d'un crime et, de manière générale, d'actions illicites ou contraires à l'ordre public ;
- Contraires aux bonnes mœurs ;
- Portant sur des Informations de la CDC ou de ses clients, au mépris de son obligation de confidentialité.

- *L'utilisateur se doit d'être vigilant pour éviter les incidents involontaires et détecter les actes de malveillance sur les ressources.*

- *Il est obligatoire de respecter la classification des informations selon leur niveau de confidentialité : un document est considéré confidentiel dès lors que sa diffusion publique pourrait porter préjudice à la CDC et/ou ses partenaires et clients (une perte financière, une perturbation du fonctionnement d'une direction, une infraction à la législation -ex : RGPD-, un possible conflit social, une perte de marchés ou d'investissement, ou un article défavorable dans les médias). L'usage des informations et des documents de la CDC ne doit pas sortir du cadre de l'activité au sein de la CDC.*

3.2 Usages de l'informatique mobile

- Il est rappelé que les équipements mobiles qui seraient mis exceptionnellement à la disposition des utilisateurs par la CDC sont la propriété de la CDC et sont destinés à être utilisés que dans le cadre de l'exécution de leurs prestations.

- Le nomadisme suppose une vigilance rigoureuse pour éviter toute perte et/ou vol des équipements de la CDC et des informations et données qui y sont stockées.

3.3 Usages de la messagerie électronique

- L'usage de la messagerie électronique par l'utilisateur n'est autorisé que dans le cadre de l'exécution de ses prestations. L'utilisateur de la messagerie électronique est clairement identifié comme étant un prestataire de service de la CDC.

- Certaines règles spécifiques sont à respecter, notamment :
  - Le contenu des messages électroniques est confidentiel ;
  - Le re-routage des messages vers une adresse de messagerie externe à la CDC (y compris toute adresse de messagerie personnelle) est strictement interdit ;
  - L'utilisateur doit faire preuve de vigilance vis-à-vis de l'identité des auteurs des messages reçus, notamment des correspondants extérieurs et veiller à ne pas ouvrir les messages et les pièces jointes qui semblent avoir une origine inconnue ou douteuse ;
  - La copie partielle ou totale ou la réutilisation de tout ou partie des listes de diffusion internes ou externes de la CDC et/ou de ses clients est interdite, sauf autorisation expresse et préalable de la CDC.

- D'une manière générale, l'utilisation de la messagerie doit être conforme à la réglementation applicable et aux prescriptions des RSSIPS et, notamment, ne doit pas porter atteinte à l'image, à la réputation, à la vie privée, à la sécurité d'autrui ou de la CDC et/ou de ses clients ni au bon fonctionnement des ressources de la CDC et/ou de ses clients.

- Pour des besoins de sécurité, la CDC peut être amenée à accéder, sur la messagerie électronique d'un utilisateur, aux messages reçus et envoyés, sans autorisation de l'utilisateur et hors la présence de ce dernier.

- Un comportement responsable et circonstancié est la meilleure protection contre toute pollution numérique, attaque visant à abuser de l'utilisateur (virus, spam, phishing, spywares, canulars…), ou fuite d'information.

- *Il est formellement interdit d'envoyer par messagerie tout document propriété de la CDC, sans l'accord formel d'un personnel de la CDC. Pour tout envoi de document propriété de la CDC vers l'extérieur, un personnel de la CDC devra obligatoirement en être destinataire ou copie.*

3.4 Usages des services Internet

- Grand vecteur d'infection, internet reste indispensable et demande d'autant plus de précautions. Pour autant, les services Internet ne doivent pas provoquer ou être des vecteurs à des fuites d'information.

- Par principe, l'accès internet est mis à la disposition des utilisateurs pour les seuls besoins de l'exécution de leurs prestations et dans les limites des droits accordés et des accès autorisés aux services internet par la CDC.

- Seuls ont vocation à être consultés les sites internet présentant un lien direct et nécessaire avec les prestations à la charge de l'utilisateur.

- De manière préventive, la CDC met en œuvre un certain nombre de dispositifs de filtrage de sites, notamment ceux dont le contenu peut être contraire à l'ordre public ou aux bonnes mœurs.

- L'utilisateur est informé des risques liés à l'utilisation des services d'échanges et de communications d'information (forums, réseaux sociaux et autres services collaboratifs). Il en résulte que l'utilisateur n'est pas autorisé à utiliser ces services collaboratifs en dehors de la stricte nécessité de ses fonctions au sein de la CDC et explicitement autorisés par la CDC (par exemple, réseau social interne à la CDC).

- *Il est formellement interdit d'uploader ou de partager tout document propriété de la CDC en utilisant les services Internet au sens large, sans l'accord formel d'un personnel de la CDC.*

3.5 Usages des services de téléphonie (fixe et mobile)

- Les postes téléphoniques qui seraient mis exceptionnellement à la disposition des utilisateurs le sont pour les stricts besoins de l'accomplissement de leurs prestations.
- Les utilisateurs sont informés que le système de téléphonie enregistre les numéros de téléphones sortants. En outre, des relevés individuels téléphoniques sont établis tous les mois, toutefois, les quatre derniers chiffres des numéros sont occultés.
- Les utilisateurs sont informés que les données relatives à l'utilisation des services de téléphonie ne sont conservées, en principe, que pour une durée maximale d'un (1) an conformément à la législation.

04

Propriété intellectuelle

- Le respect de la propriété intellectuelle, des droits d'auteur, et de la conformité des licences logicielles est essentiel.

- Sauf autorisation expresse et préalable de la CDC, le téléchargement et l'installation de logiciels par l'utilisateur sont interdits.

- Il est rappelé à l'utilisateur que les œuvres de l'esprit telles que les logiciels, photographies, images, bases de données, œuvres audiovisuelles et musicales, fichiers textes (études, mémo, consultations, analyses, notes de tout type, schémas, dossiers, maquettes) marques, dessins et modèles, noms de domaine et autres signes distinctifs, etc. sont protégées par le droit de la propriété intellectuelle.

- L'utilisateur ne doit donc pas utiliser les ressources en portant atteinte aux droits de la propriété intellectuelle de la CDC, de ses clients ou de tiers.

- *L'utilisateur s'interdit toute reproduction, représentation, publication, exploitation et/ou utilisation de fichiers, données, logiciels ou bases de données de tiers protégés par le droit de la propriété intellectuelle ou un droit privatif en dehors des possibilités légales ou contractuelles qui lui sont reconnues.*

05

Protection de l'information et des données à caractère personnel

- Toutes les dispositions organisationnelles et techniques de protection de l'information, en particulier de protection des données à caractère personnel, ne remplaceront jamais la vigilance humaine qui reste primordiale.

- L'utilisateur a une obligation générale et permanente de confidentialité et de discrétion attachée à l'utilisation des informations, données et documents électroniques disponibles sur le SI de la CDC et/ou de ses clients, et ce, pour la sauvegarde du patrimoine et des intérêts de la CDC et/ou de ses clients, mais également des personnes concernées par ces informations, données ou documents (partenaires, clients, fournisseurs, personnels de la CDC, bénéficiaires, etc.).

- L'utilisateur veille tout particulièrement à préserver la sécurité (Disponibilité, Intégrité, Confidentialité, Preuve) des données à caractère personnel auxquelles il a accès afin, notamment, de mettre la CDC en mesure de respecter les dispositions du Règlement européen (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ainsi que la loi n°78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés, qui oblige à prendre toutes précautions utiles afin de préserver la sécurité desdites données et d'empêcher en particulier qu'elles ne soient déformées ou endommagées ou que des tiers non autorisés y aient accès.

06

Contrôle de l'usage des ressources

- Des mesures de contrôle et de suivi sont mises en œuvre dans le respect des principes de transparence et de proportionnalité des moyens de collecte, ceci à des fins de sécurité, de protection et de vérification du bon accès et usage des ressources.

- Ces mesures ont pour finalités :
  - de garantir le bon fonctionnement de ces ressources,
  - de contrôler le respect des règles d'utilisation et de sécurité du SI de la CDC et de ses clients,
  - de pouvoir identifier et, le cas échéant, sanctionner des usages contraires aux législations et réglementations applicables,
  - de pouvoir répondre aux requêtes des autorités publiques habilitées (services de police, autorités judiciaires…).

- Les données et traces informatiques enregistrées dans le cadre de ces mesures portent sur l'identification du compte de l'utilisateur, la date et heure de l'action considérée, la nature et les résultats de l'action. Ces données et traces informatiques sont conservées pendant une période maximale de 18 mois (sauf obligations légales ou règlementaires particulières de conserver ces données sur une durée plus longue, ex : délais de prescription) et font l'objet de mesures de protection adéquates contre le risque de divulgation et d'utilisation abusive.

- En complément, ces données et traces informatiques font l'objet de traitements automatisés à des fins statistiques (nombre de messages émis vers ou reçus de l'Internet, volumes occupés par l'ensemble des boîtes aux lettres, sites Internet les plus visités, fréquence d'accès à l'internet ou à l'Intranet, nombre de pages visitées, nature des pages visitées, date heure et durée de connexion, taille des espaces sur les serveurs de fichiers, durées totales des connexions distantes, etc.).

- Lorsque les circonstances l'exigeront (évènements menaçant l'intégrité et la sécurité du SI de la CDC et/ou de ses clients), que la responsabilité ou les intérêts de la CDC et/ou de ses clients seront en jeu, les moyens d'investigation nécessaires seront mis en œuvre, par la CDC, et le cas échéant, l'accès aux ressources du SI de la CDC et/ou de ses clients pourra être restreint, voire fermé, sans préavis.

- En cas de risque pour le SI de la CDC et/ou de ses clients et/ou d'usage inapproprié des ressources de la CDC et/ou de ses clients, des poursuites pourront être engagées contre l'utilisateur concerné, notamment sur la base de ces données de connexion.

07

Serveurs de fichiers

Confidentiel

- Les contenus fournis dans le cadre de l'exécution des prestations doivent être stockés et partagés sur les serveurs de fichiers du réseau interne, selon les instructions de la CDC.

- Les utilisateurs ne doivent en aucun cas utiliser ces espaces et les serveurs partagés de façon générale pour stocker et/ou partager tout fichier, document, données (notamment musiques, photos, vidéos) sans rapport avec l'exécution des prestations. Tout contenu stocké au mépris de cette interdiction pourra être supprimé sans délai et sans avertissement préalablement de l'utilisateur.

08

Mention d’information : données à caractère personnel

- Le Règlement européen (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ainsi que la loi n°78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés, définissent les conditions dans lesquelles des traitements de données à caractère personnel peuvent être opérés.

- La réglementation relative à la protection des données à caractère personnel interdit notamment toute collecte et traitement de données à l'insu des personnes concernées, et vise également à préserver la confidentialité, la sécurité et l'intégrité des données à caractère personnel contenues dans les traitements opérés, lesquels doivent respecter une finalité déterminée, et légitime.

- Dans le cadre des présentes RSSIPS, des traitements de données à caractère personnel issus des systèmes d'informations de la CDC et des ressources sont ainsi effectués au sein de la CDC concernant les utilisateurs, notamment dans le cadre des systèmes de contrôle prévus dans les RSSIPS, ceci dans le respect de la règlementation précitée. La CDC s'engage à ce que les données concernant les utilisateurs soient collectées et traitées de manière loyale et licite, dans les conditions exposées.

- La CDC, responsable de traitement, poursuit son intérêt légitime et met ainsi en œuvre des traitements de données à caractère personnel en relation avec l'usage de ses systèmes d'information et des ressources couverts par les présentes RSSIPS et pour assurer leur sécurité.

- Plus précisément, ces données collectées auprès des utilisateurs sont obligatoires aux fins de mise à disposition de moyens informatiques et de communication nécessaires à la réalisation des prestations qui leur sont confiées, de bonne gestion, de maintenance, d'organisation et de sécurité des systèmes d'information et des ressources.

- Les données collectées sont conservées pendant toute la durée des relations commerciales et contractuelles augmentée de la durée des prescriptions légales, à l'exception des données et traces informatiques relatives aux contrôles de l'usage des ressources qui sont conservées pendant une période maximale de 18 mois (sauf obligations légales ou règlementaires particulières de conserver ces données sur une durée plus longue).

- Des données vous concernant sont susceptibles d'être transférées en dehors de l'Union européenne (vers les Etats-Unis), dans le cadre de l'utilisation d'outils de communication informatique et de messagerie électronique édités par Microsoft et mis à votre disposition au sein de la CDC. Ces transferts sont encadrés par des clauses contractuelles types de la Commission européenne.

- Les données collectées sont destinées aux services concernés de la CDC en charge de la sécurisation des systèmes d'information de la CDC ou qui seraient légitimes à recevoir ces données, sur la base d'habilitations strictes et d'un accès restreint, ainsi que, le cas échéant, à ses sous-traitants ou prestataires mandatés aux mêmes fins.

- En application de la réglementation en vigueur, l'utilisateur dispose d'un droit d'accès, de rectification ou d'effacement, de limitation du traitement de ses données, d'un droit d'opposition, ainsi que du droit de définir des directives relatives au sort de ses données après son décès, qui s'exercent par courrier électronique à mesdonneespersonnelles@caissedesdepots.fr ou par courrier postal à l'adresse suivante : Caisse des Dépôts et consignations – Données Personnelles - Établissement de Bordeaux – 5 rue du Vergne – 33059 BORDEAUX CEDEX

- Pour toute information complémentaire ou difficulté relative à l'utilisation de vos données, vous pouvez contacter notre Déléguée à la protection des données (DPO) à l'adresse : dpo@caissedesdepots.fr

- En cas de difficulté non résolue, vous pouvez saisir la Commission Nationale de l'Informatique et des Libertés (CNIL), autorité de contrôle en charge du respect des obligations en matière de données à caractère personnel.

***

Annexe

Modèle d'attestation de respect des règles de sécurité des systèmes d'information de la CDC par l'intervenant

Je, soussigné, [NOM, PRENOM, ADRESSE]

Intervenant pour le compte de la société prestataire [DENOMINATION SOCIALE + RCS]

Atteste avoir été informé par la société prestataire des règles de sécurité des systèmes d'information de la CDC pour les prestataires de service (dites RSSIPS), en avoir pris connaissance et m'engage à respecter les obligations qu'elles contiennent.

Date ……..

Signature……