Code de conduite

relatif à la sécurité et la gestion de l'information

HARDIS GROUP

Classification Hardis Group : **Publique C4**

Sommaire

Introduction et objectifs

Le présent code porte sur les obligations en matière de sécurité, sur la gestion de l'information et sur l'utilisation des ressources de Hardis Group et ses filiales (ci-après dénommé le « Code »).

Le terme générique « Hardis Group » désigne Hardis Group et ses filiales.

Ce Code s'applique à toute personne ou entité réalisant des prestations de service pour Hardis Group, ainsi qu'à leur personnel et sous-traitant le cas échéant.

Il vient compléter les obligations découlant du ou des contrat(s) conclu(s) avec votre société en précisant vos droits et devoirs spécifiques afin d'assurer votre conformité au regard des règles en matière de sécurité de l'information lors de l'exécution des prestations qui vous sont confiées (ci-après dénommées les « Activités »).

01

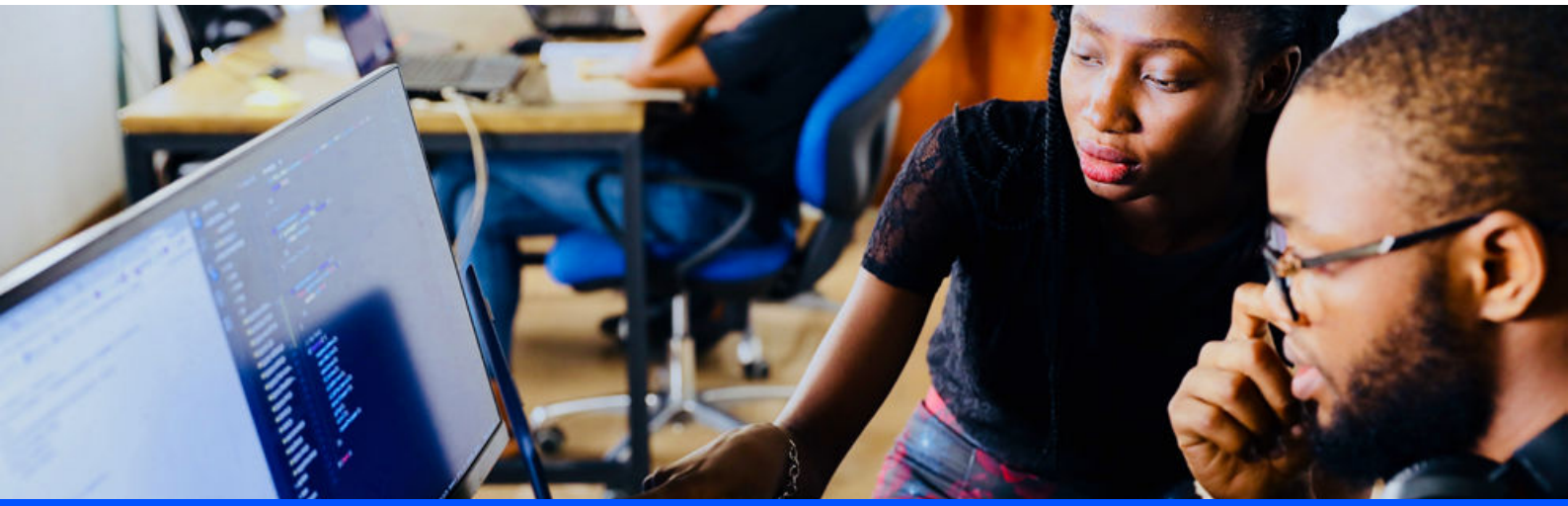
Conformité aux lois et réglements

Pour la durée de la relation, vous déclarez que vous êtes et vous demeurerez conformes à toutes les lois et réglementations, et en particulier au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après, le « RGPD ») et vous vous engagez à imposer des obligations identiques à votre personnel ainsi qu'à tous tiers sous votre contrôle (y compris vos sociétés affiliées, intervenants et sous-traitants, s'il en existe). Sauf disposition particulière, vous vous engagez à ce que la localisation des données de Hardis Group soit en France ou à minima au sein de l'Union Européenne.

Le non-respect de ces dispositions p ourra entraîner la résiliation immédiate du ou des contrats conclus entre Hardis Group et votre société.

De plus, Hardis Group se réserve le droit d'effectuer un audit une fois par an sur le périmètre des Activités confiées sous réserve d'un préavis de 15 jours Vous vous engagez à assister et coopérer pleinement avec Hardis Group lors de l'audit.

Vous vous engagez également à assurer un devoir de conseil auprès de Hardis Group et à protéger les informations confidentielles ou les données à caractère personnel reçues et ne jamais utiliser ces informations pour en tirer un quelconque avantage.



02

Dispositions générales sur la sécurité

2.1. Sécurité liée aux ressources humaines

Vous vous engagez à gérer l'identité et les mouvements (départs, arrivés, mobilités, etc.) de votre personnel ainsi que tous tiers sous votre contrôle, de manière individuelle et unique et à gérer l'affectation des privilèges en fonction du poste et de la mission de la personne concernée et du principe du moindre privilège.

Vous vous assurez également du respect des droits en matière de confidentialité en faisant signer un accord de confidentialité spécifique à votre personnel s'il assure des activités d'administration (droits à privilèges) ou traite des données à caractère personnel sensibles ou hautement personnelles telles que définies par la réglementation. Ce principe s'applique également pour les tiers sous votre contrôle (sous-traitants, intervenants, etc.).

Vous veillez à l'adéquation des compétences de vos collaborateurs et de leur nombre, notamment en assurant les formations et sensibilisations adéquates.

Dans le cadre de ces obligations, lorsque la réglementation le permet, vous acceptez de vous soumettre à une demande d'information ou d'extrait de casier judiciaire pour le personnel qui traitera des données sensibles ou confidentielles pour Hardis Group.

2.2. Sécurité et contrôle d'accès

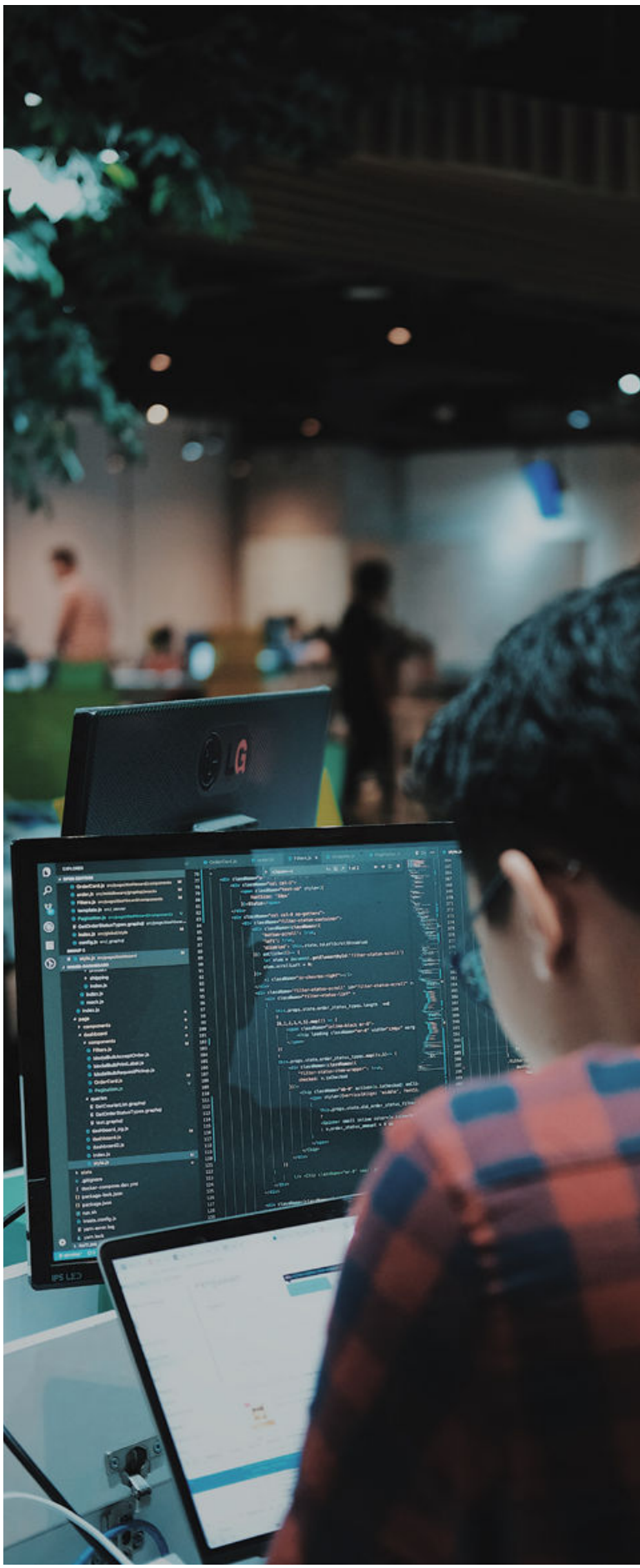
Vous vous engagez à effectuer un contrôle d'accès et à identifier individuellement et nominativement chaque personne ayant un accès aux données et aux applications relatives aux Activités confiées à votre société par Hardis Group.

Notamment, vous vous engagez à ce que vos locaux soient protégés contre les accès non autorisés et que vos Data Centers soient certifiés ISO27001.

Vous appliquez toutes les mesures de sécurité adéquates en matière de sécurité des équipements, des communications et des locaux conformément aux règles de l'art en la matière.

2.3. Gestion des actifs

Vous vous engagez à gérer les actifs relatifs aux Activités confiées à votre société, en cohérence avec les besoins exprimés par Hardis Group que ce soit en termes de disponibilité, d'intégrité, de confidentialité et de traçabilité de l'information traitée. Vous vous engagez également à restituer les actifs (patrimoine matériel et immatériel, y compris les informations confidentielles ou données à caractère personnel) de Hardis Group dans le cadre d'une fin de service et à supprimer toutes les données confiées puis d'en informer formellement Hardis Group.



03

Pratiques en matière de cyber sécurité

3.1. Protection contre les codes malveillants

Vous vous engagez à avoir déployé sur votre parc un logiciel de lutte contre les virus et codes malveillants dont la base de référence est à jour (liste OWASP).

Vous vous engagez également à avoir les contrats de maintenance, ainsi que les moyens nécessaires au maintien en condition opérationnelle et de sécurité des actifs.

Vous appliquez les correctifs recommandés par vos fournisseurs de solutions matérielles ou logicielles sur tous les matériels dont vous avez la charge.

Vous utiliserez des fonctions crypto-graphiques répondant aux préconisations des documents de référence de l'ANSSI à chaque fois que cela sera nécessaire.

3.2. Sauvegarde et continuité d'activité

Dans le cadre des Activités confiées à votre société, vous vous engagez à prendre toutes les mesures qui s'imposent en matière de sauvegarde et de restauration afin de protéger les données stockées. Notamment, vous prenez l'engagement de conserver les données de Hardis Group uniquement dans le cadre des Activités confiées et de n'en pratiquer aucun autre usage.

Vous vous engagez également à protéger les sauvegardes contre les défauts d'intégrité, de disponibilité et confidentialité et à réaliser des tests de restauration de sauvegarde régulièrement ou à la demande d'Hardis Group et d'en assurer un reporting.

Vous avez réalisé un plan de continuité d'activité afin de satisfaire au niveau de service fixé sur les Activités confiées.

3.3. Développement et maintenance

Vous vous engagez, notamment pour toute activité de développement applicatif, à appliquer et contrôler la bonne application de référentiel adapté à la technologie utilisée et à considérer les exigences de sécurité issues du RGPD à chaque étape du cycle de vie du logiciel ou de la solution, et à avoir la validation écrite de Hardis Group avant toute modification d'un objet en production (processus de retour en arrière décrit et validé).

Vous suivez les publications de corrections de sécurité par les éditeurs sur le périmètre des Activités confiées et mettez en œuvre de manière systématique un processus de gestion du changement et de configuration, considérant les exigences de sécurité et issues du RGPD pour toute mise en production.

3.4. Gestion des incidents et vulnérabilités

Vous avez un devoir d'alerte auprès de Hardis Group pour toute identification de situation possiblement génératrice d'incident de sécurité.

Vous vous engagez donc à assurer, sur le périmètre des Activités confiées, la détection des incidents, l'analyse des éléments remontés, la qualification et la détermination d'un plan d'action ainsi que la traçabilité des actions (journalisation des actions des utilisateurs) pouvant avoir un impact sur la sécurité, afin de réagir au plus tôt lors de la détection d'un événement sensible pour la sécurité du système.

Vous vous assurez d'appliquer les correctifs sur les systèmes avec une périodicité adaptée au niveau de criticité du serveur, à minimiser les services accessibles, à avoir une politique de suppression des éléments non-indispensables (services, comptes inutiles, etc.) et à respecter une politique de mot de passe conforme aux préconisations de l'ANSSI.

Vous vous engagez également à appliquer sur le périmètre des Activités confiées, un plan de gestion de crise (intervenants, mode opératoire de qualification, alerte traitement et sortie de crise, les moyens utilisés/ mobilisables en cas de crise, etc.).

3.5. Relation avec les tiers

Les Activités confiées à votre société ne sont soumises à une co-traitance / sous-traitance qu'avec l'accord préalable de Hardis Group. En cas de co-traitance ou de sous-traitance vous vous engagez à garantir le niveau de conformité aux exigences de la présente annexe auprès des co-traitants ou sous-traitants concernés.

04

Utilisation des ressources de Hardis Group

4.1. Règles générales relatives à l'utilisation des ressources en matière de systèmes d'information

Dans le cadre des Activités confiées à votre société, il est possible que vous ayez accès au système informatique de Hardis Group (ci-après dénommés les « Ressources »).

L'ensemble des moyens et Ressources mis à votre disposition demeure la propriété de Hardis Group ou celle de ses donneurs de licence. Afin d'assurer la sécurité des systèmes d'information, cet accès aux Ressources est temporaire et révocable à tout moment à l'entière discrétion de Hardis Group. Les appareils qui vous seront fournis dans ce cadre devront être restitués sans délai dans le cas où Hardis Group supprimerait l'accès aux Ressources, ou dans le cas où les Activités confiées viendraient à prendre fin pour quelque raison que ce soit, ou en cas de modification de tout ordre de mission et que le nouveau service ne nécessite plus de recourir aux Ressources.

Vous ne devrez, pour accéder aux Ressources, utiliser que celles mises à votre disposition ou autorisées par Hardis Group. Vous ne devrez pas enfreindre les règles de confidentialité en vigueur au sein de Hardis Group ou agir de manière à placer Hardis Group dans une situation délicate.

Chacun des salariés de votre société participant aux Activités se verra délivrer à titre individuel des identifiants de connexion lui permettant d'avoir accès aux Ressources ; en aucun cas ces identifiants ne devront être communiqués à une autre personne physique ou morale.

Il vous appartiendra de signaler de manière systématique (**security.alert@hardis-group.com**) tout incident ou événement sortant de l'ordinaire dont vous pourrez être amené à être témoin dans le contexte des Activités.

4.2. L'utilisation d'Internet

Dans le cadre de l'accès aux Ressources de Hardis Group et notamment d'une connexion à Internet, vous êtes seul responsable de l'utilisation que vous en faites et plus particulièrement du choix des sites que vous visitez, ces derniers devant avoir un lien avec les Activités. Vous devez veiller à ne pas perturber le bon fonctionnement des Ressources en faisant une utilisation inappropriée ou excessive d'Internet telle que : non-respect des droits d'auteur, téléchargement de logiciels ou de fichiers non autorisés ou non conformes à la législation et aux bonnes mœurs, téléchargement de fichiers volumineux à des fins personnelles, consultation de dossiers à contenu non-professionnel notamment en mode streaming, etc.

Seuls ont vocation à être consultés les sites Internet présentant un lien direct avec votre activité professionnelle, une utilité au regard de vos fonctions exercées ou de vos missions à mener.

Une consultation ponctuelle du web pour un motif personnel dans des limites raisonnables est tolérée, dès lors que le contenu des sites Internet consultés n'est pas contraire à l'ordre public et aux bonnes mœurs et ne met pas en cause l'intérêt et la réputation de Hardis Group.

4.3. La messagerie électronique

La messagerie électronique est un outil essentiel pour les activités quotidiennes. Comme toute sorte d'informations (plus ou moins confidentielles) peuvent y transiter, il est essentiel que vous respectiez les recommandations suivantes pour en assurer la sécurité.

Vous serez seul responsable du contenu des messages que vous enverrez ou transmettrez après les avoir reçus et de leur destination. Vous devrez être attentif à ne pas perturber le fonctionnement général des outils par le biais d'une utilisation abusive ou inappropriée de la messagerie électronique : sauvegarde d'un nombre excessif de messages, envoi à des destinataires multiples, envoi de pièces jointes alors que cela n'est pas nécessaire, envoi de pièces jointes/de fichiers trop lourds ou sous un format non compressé, communication de renseignements confidentiels par des voies non sécurisées, etc.

Vous devrez rester vigilant quant au contenu des emails et des pièces jointes non sollicitées, tels que notamment emails de « phishing » ou éventuels logiciels malveillants (malware).

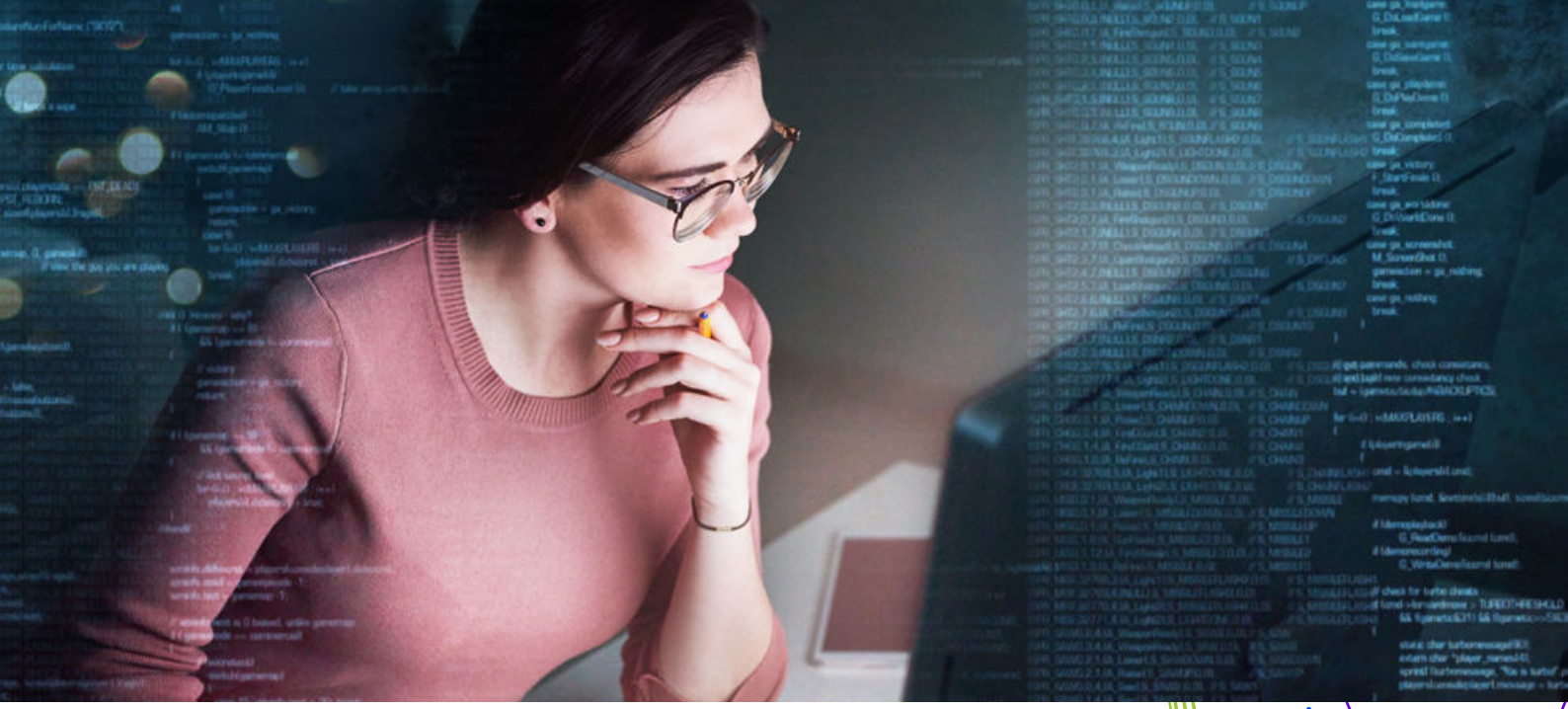
4.4. Les espaces de stockage et la protection des connexions

Les espaces de stockage doivent être sécurisés pour respecter les engagements en matière de confidentialité et de protection des données de Hardis Group.

Les périphériques informatiques mis à votre disposition par Hardis Group sont approuvés par l'équipe en charge du système d'information (SI). L'usage de tout autre périphérique informatique, fixe ou mobile, dans le cadre des Activités doit être préalablement déclaré auprès de cette même équipe.

L'accès aux éléments du SI (sessions sur les postes de travail, applications, messagerie électronique ou téléphonique, etc.) est protégé par des paramètres de connexion (identifiants, mots de passe) dont il est primordial de respecter les règles de conservation ainsi que les recommandations d'Hardis Group en matière de gestion des mots de passe.

Vous êtes responsable de l'usage que vous faites des Ressources de Hardis Group, vous devez donc assurer, à votre niveau, la sécurité de ces dernières et vous vous engagez à ne pas volontairement mettre en péril leur intégrité et le fonctionnement normal du réseau.



05

Sanctions en cas de non-application du code

En cas de non-respect des règles définies par le présent Code, si vous aviez un accès aux Ressources, leur utilisation sera suspendue ou restreinte, sans préjudice du droit pour Hardis Group de procéder à la résiliation anticipée pour violation de la part de votre société de tout contrat relatif aux Activités.

De plus, l'engagement de votre responsabilité civile ou pénale pourra être recherché à l'initiative de Hardis Group ou de tous tiers autorisés.

Les règles définies par le Code constituent les règles fondamentales que vous vous engagez à respecter. Nous attirons toutefois votre attention sur leur absence de caractère exhaustif, celles-ci s'appliquant sans préjudice du respect des lois et réglementations applicables par ailleurs.