DOCUMENT PORTANT POLITIQUE DE SÉCURITÉ OU DE LA CHARTE INFORMATIQUE

2022

Table des matières

1 Préambule

La présente charte définit les conditions d'utilisation et les règles de bon usage des ressources informatiques de REVELATEUR SARL conformément au règlement et à la législation en vigueur. REVELATEUR SARL est une société spécialisée dans les prestations numériques plus précisément dans le domaine de l'enseignement. C'est une plateforme sur laquelle se trouvent des données personnelles des apprenants afin de permettre leur suivi scolaire.

Objet de l'activité de la société. Prestations de services numériques et autres activités liées au numérique

La présente politique constitue le cadre général concernant les accès, l'utilisation et la sécurité des technologies de l'information de REVELATEUR. Elle oriente les comportements attendus des usagers quant à l'utilisation du matériel informatique, des logiciels, les accès et l'utilisation du réseau informatique.
Cette politique permet de préserver la confidentialité, la disponibilité, l'intégrité et la valeur des biens.

La présente politique de sécurité a pour but de sensibiliser les utilisateurs sur les risques qui menacent la sécurité du système d'information en déterminant les droits et obligations de chacun. Elle vise également à rappeler les règles de bon usage du système d'information à des fins exclusivement professionnelles, sauf exception prévue dans la présente charte. Ces règles sont valables pour tous les supports et outils de transmission de l'information utilisés, que ce soit notamment avec l'ordinateur, les tablettes et autres terminaux mobiles, les clés USB, le téléphone (fixe ou mobile), le télécopieur, l'Intranet, l'Internet, la visio-conférence, les connexions WIFI et la messagerie électronique. Le système d'information comprend également les matériels personnels que l'utilisateur pourrait être amené à utiliser dans le cadre de son activité professionnelle.

Les usages des ressources informatiques non conformes aux préconisations de la présente charte peuvent être constitutifs de fautes professionnelles susceptibles d'entraîner pour l'utilisateur des sanctions disciplinaires.

Aussi, dans un but de transparence à l'égard des utilisateurs, de promotion d'une utilisation loyale, responsable et sécurisée du système d'information et des équipements informatiques, la présente charte pose les règles relatives à l'utilisation de ces ressources.

2 Définitions

« *Equipements informatiques* » : désigne l'ensemble des matériels, équipements, outils informatiques mis à disposition par REVELATEUR aux Utilisateurs.

« *Personnes concernées* » : désigne les personnes physiques dont les données à caractère personnel sont traitées par REVELATEUR ou par tout tiers via le système d'information ou de communication de REVELATEUR, ou via des Equipements informatiques.

« *Utilisateurs* » : désigne toute personne qui utilise les systèmes d'information de REVELATEUR et les Equipements informatiques quel que soit son statut, et notamment les mandataires sociaux, les salariés, les intérimaires, les prestataires personnes physiques, les prestataires personnes morales, les stagiaires, les employés de sociétés prestataires, les visiteurs occasionnels, les salariés suivis et de manière générale, à toute personne qui a obtenu un droit d'utilisation du système d'information de REVELATEUR] ou de ses Equipements informatiques.

3 Cadre Normatif

La présente Politique de sécurité est soumise à la législation en vigueur en République du Bénin notamment :

- Loi n°2017 -20 du 20 avril 2018 portant code du numérique en République du BENIN ;
- Les décrets d'application de la loi n°2017 -20 du 20 avril 2018 portant code du numérique en République du BENIN ;

4 Champ d'application

4.1 Personnes visées

Les obligations décrites dans la présente charte s'appliquent à toute personne qui utilise les systèmes d'information de REVELATEUR quel que soit leur statut, y compris les stagiaires, employés de sociétés prestataires, visiteurs occasionnels.
Les salariés, consultants internes ou externes et autres prestataires de services de la société veillent à faire respecter les règles posées dans la présente charte à toute personne à laquelle ils permettraient d'accéder au système d'information et de communication.

La présente charte sera annexée aux contrats conclu avec les personnes intervenant dans l'activité de la société ainsi qu'au contrat conclu avec des tiers concernant l'informatique dans le cadre d'un contrat de sous-traitance.

4.2 Accès par des tiers aux systèmes d'information

Tout utilisateur extérieur ne peut avoir accès aux systèmes d'information de la société que moyennant une autorisation expresse préalable délivrée par le Directeur des Systèmes d'Information et s'engage, dès lors, à respecter l'ensemble des dispositions de la présente charte.

4.3 Dérogations possibles

Toute demande de dérogation aux différents éléments définis dans le cadre de la présente Charte doit être présentée par écrit au Directeur des Systèmes d'Information (DSI). La décision finale est ensuite prise en concertation avec l'instance décision décisive de la société qui se réserve le droit d'accepter ou de refuser les demandes de dérogation.

5 Objectifs de la politique de sécurité

Cette politique de sécurité vise les objectifs suivants :

- assurer que les utilisateurs observent les bonnes pratiques et les règles quant à l'utilisation des technologies de l'information;
- assurer que les normes en matière de sécurité informatique soient dûment mises en application ;
- réviser périodiquement les résultats des vérifications et contrôles, notamment pour y relever les anomalies et autres incidents ;
- recommander les actions à prendre pour corriger les situations anormales ou dangereuses, notamment, les processus opérationnels et les grandes stratégies en matière informatique et les achats d'équipements ;
- informer la Direction des travaux, activités et incidents en matière de sécurité informatique.
- assurer que les éléments opérationnels qui requièrent une approbation des différentes Directions soient respectés.

6 Utilisation des systèmes d'information et des outils de communication

6.1 Accès

L'accès aux éléments du système d'information comme la messagerie électronique ou téléphonique, les sessions sur les postes de travail, le réseau, certaines applications ou services

interactifs est protégé par des paramètres de connexion (identifiant, mot de passe) individuels attribués à chaque utilisateur.

Ces paramètres sont personnels à l'utilisateur et doivent être gardés confidentiels. Ils permettent en particulier de contrôler l'accès des utilisateurs. Ils ne doivent ni être communiqués à son responsable hiérarchique, ni à un tiers. Ces paramètres doivent être mémorisés par l'utilisateur ; l'utilisateur ne doit les conservés, sous quelque forme que ce soit. En tout état de cause, ils ne doivent pas être transmis à des tiers.

Chaque utilisateur est responsable des opérations informatiques, locales ou distantes, faites à partir des ressources qui lui sont allouées. Il doit donc prendre les précautions suivantes :

- garder secrets ses mots de passe ;
- ne jamais quitter son poste de travail sans en protéger l'accès (verrouillage d'écran) ;
- informer les responsables sécurité des tentatives de violation de son compte et, de façon générale, de toute anomalie qu'il constate ;
- choisir des mots de passe suffisamment robustes (combinaison de lettres en minuscules, majuscules, chiffres, caractères spéciaux, absents du dictionnaire et sans lien évident avec l'utilisateur).

6.2 La messagerie électronique

Chaque salarié dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique. Les utilisateurs doivent respecter les règles d'usage suivantes :

- faire un usage raisonné de la messagerie et ne pas surcharger les boîtes de messagerie internes ou externes ;
- ne pas diffuser des courriels de type chaînes de messages, escroquerie, jeux, paris,... ;
- ne pas utiliser leur adresse électronique professionnelle sur des sites internet (groupes de discussion, chats, commerce, forums, blogs, etc...), sans rapport avec l'activité professionnelle ;
- ne pas rediriger manuellement ou automatiquement les messages professionnels qu'ils reçoivent sur leur messagerie professionnelle vers une messagerie personnelle ;
- s'assurer, à chaque envoi de données, en particulier sensibles, que la liste de diffusion ne comporte pas de destinataire inapproprié ;
- ne pas ouvrir les messages douteux et les pièces jointes suspectes, ne pas répondre aux émetteurs de tels messages et ne pas cliquer sur les liens présents dans ces messages (même s'ils se présentent comme des liens de « désabonnement ») ;
- prévenir l'assistance informatique en cas de doute ou après avoir ouvert un message ou cliqué sur un lien qui s'avère a posteriori douteux.

L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même valeur qu'un courrier manuscrit et peut rapidement être communiqué à des tiers. Il convient, pour chaque utilisateur, de prendre garde au respect d'un certain nombre de principes, afin d'éviter les dysfonctionnements du système d'information, de limiter l'envoi de messages non sollicités et de ne pas engager la responsabilité civile ou pénale de la société et/ou sa propre responsabilité.

Les utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne doivent pas comporter d'éléments illicites de nature contrefaisantes ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire ni comporter des propos diffamatoires ou injurieux.

6.3 Utilisation

Les systèmes d'information mis à disposition des utilisateurs sont réservés à un usage professionnel exclusif. Tout usage des moyens informatiques et de communication électronique

est réputé avoir été réalisé par le bénéficiaire de l'identification d'accès et ce, à des fins professionnelles.

Par ailleurs et indépendamment des dérogations possibles précitées, une utilisation des systèmes d'information à des fins personnelles peut être résiduelle. Ainsi, tant dans la fréquence que dans la durée, elle ne peut être envisagée qu'en dehors du temps de travail et de manière limitée pendant le temps de travail, conformément à la Jurisprudence en la matière. Les répertoires informatiques et échanges électroniques doivent alors porter la mention **« privé » ou « personnel ».** L'employeur se réserve le droit de limiter ou suspendre une telle utilisation, en cas d'abus.

En cas de manquement à ces règles, les répertoires informatiques et échanges électroniques sont présumés être à caractère professionnel.

Toutefois, les utilisateurs sont invités à utiliser leur messagerie personnelle pour l'envoi de messages à caractère personnel plutôt que la messagerie de l'entreprise.

7 Internet / Intranet

Dans le cadre de leur activité, les utilisateurs peuvent avoir accès à internet pour leur permettre d'assurer au mieux leur mission. Afin d'assurer le respect des obligations qui lui incombent dans ce cadre, la société met en place :

- des dispositifs de filtrage des accès à internet, qui limitent l'accès aux seules catégories de sites autorisés ;
- des mécanismes de collecte des informations de connexion des utilisateurs à internet.
- des configurations du navigateur et la restriction de téléchargement de certains fichiers.

Les Utilisateurs ne doivent en aucun cas se livrer à une activité illicite ou portant atteinte aux intérêts de la société, y compris sur internet.

En particulier, sont interdits :

- L'utilisation de l'internet à des fins commerciales personnelles en vue de réaliser des gains financiers ou de soutenir des activités lucratives.
- la création ou la mise à jour au moyen de la connexion mise à disposition par la société de tout site internet, notamment des pages personnelles.
- la connexion à des sites internet dont le contenu est contraire aux lois, aux règlements, à l'ordre public, aux bonnes mœurs ou à l'image de marque de l'entreprise, ainsi qu'à ceux pouvant comporter un risque pour la sécurité du système d'information de la société ou engageant financièrement celle-ci.

8 La téléphonie

Pour leur activité professionnelle, les utilisateurs peuvent disposer d'un téléphone fixe et/ou mobile, d'un smartphone, d'une tablette ou d'une clé 3G, 4G ou plus, ou hot spot wifi.

Concernant l'utilisation des terminaux mobiles en connexion pour accès à des sites internet ou à la messagerie électronique, les règles édictées dans la présente charte s'appliquent identiquement.

De plus, il est rappelé que l'envoi de SMS est réservé aux communications professionnelles et qu'il engage la responsabilité de l'émetteur au même titre que l'envoi d'un courriel.

Les utilisateurs sont informés que les relevés de communication peuvent faire l'objet d'un contrôle.

9 Accès au système d'information en dehors du service (télétravail, en entreprise, centre mobile, … accès au bureau distant)

Le présent article concerne l'utilisation des systèmes d'information de REVELATEUR, de ses ressources, et des moyens de communication par l'utilisateur lorsque celui-ci est situé en-dehors du site physique de la société.

En premier lieu, il convient de préciser que l'ensemble des dispositions de la présente charte sont applicables aux utilisateurs accédant aux systèmes d'information et de communication de REVELATEUR à distance.

La société veille à souscrire aux assurances nécessaires pour la protection des moyens informatiques et de communication électronique mis à disposition.

Tout accès à distance par du matériel informatique personnel est interdit sauf autorisation expresse et écrite de la part du Directeur des Systèmes d'Information.

10 Données personnelles à caractère sensible

La Loi n°2017-20 du 20 avril 2018 portant Code du numérique en République du Bénin définit les conditions dans lesquelles des traitements de données à caractère personnel peuvent être opérés et institue au profit des Personnes Concernées des droits que la présente charte vise également à protéger et respecter, tant à l'égard des utilisateurs que des tiers.

A cet égard, dans un premier temps, la Direction des Systèmes d'information (DSI) interdit aux Utilisateurs :

- l'usage des données à caractère personnel auxquelles ils peuvent accéder à des fins autres que celles prévues par leurs attributions ;
- toute copie de ces données sauf si cela est nécessaire à l'exécution de leurs fonctions et dans ce cas sur préalable autorisation supérieur direct ;
- de ne pas accéder, tenter d'accéder ou supprimer les données en dehors de leurs attributions ;
- de divulguer des données à des personnes qui ne sont pas dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;

Dans un second temps, la Direction des Systèmes d'information (DSI) invite les utilisateurs aux fins :

- de prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de leurs attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- de prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;
- d'assurer, dans la limite de leurs attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
- de respecter les droits des personnes concernées (droit d'accès, de rectification, d'opposition, effacement…) conformément aux dispositions du Code du numérique et aux procédures mises en place par la société ;
- en cas de cessation de leurs fonctions, de restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données ;
- de respecter l'ensemble des procédures liées à la protection des données mises en place par la société, et à respecter et favoriser l'ensemble des mesures techniques et organisationnelles mises en place par la société afin de se conformer à la réglementation applicable ;
- d'assurer, de concert avec la Direction Générale, la Direction des Systèmes d'Information et la Direction Juridique, la formation régulière de l'ensemble du personnel et des prestataires et autres sous-traitants sur la protection des données à caractère personnel.

Conformément au code du numérique en vigueur en République du Bénin, le Directeur des Systèmes d'Information s'engage, et par voie de conséquence les utilisateurs, par le respect de la présente charte, à respecter les principes fondamentaux de la protection des données à caractère personnel, à savoir notamment la minimisation de la collecte et la préservation de la confidentialité, de l'intégrité et de la sécurité des données à caractère personnel.

Les utilisateurs sont au cœur de la protection des données à caractère personnel, et par conséquent des libertés et de la vie privée des personnes concernées. Ils sont à cet effet soumis à une obligation de confidentialité matérialisée par un engagement.

11 Secret et confidentialité – transmission d'informations

Le respect de la confidentialité des données est une exigence essentielle.

La sauvegarde des intérêts de la société nécessite le respect d'une obligation générale et permanente de confidentialité et de secret professionnel, à l'égard des données disponibles mises à la disposition de l'utilisateur pour l'exercice de son activité professionnelle dans le cadre notamment de l'utilisation des systèmes d'information, mais aussi de tout traitement.

En conséquence, l'utilisateur s'engage au respect de la présente charte, comme des textes en vigueur et notamment à veiller à ce que les tiers non autorisés n'aient pas connaissance de telles informations, conformément aux règles d'éthique professionnelle ou de déontologie, le cas échéant.

Les administrateurs des systèmes informatiques sont tenus au secret professionnel et ne doivent pas divulguer des informations ayant un caractère nominatif, de quelque nature qu'elles soient et ce, quel que soit l'ordre hiérarchique. En aucun cas, les administrateurs ne peuvent être contraints de divulguer ces informations sauf disposition législative et/ou réglementaire particulière en ce sens. En cas de non-respect de ces dispositions par les administrateurs, ceux-ci s'exposent à des sanctions disciplinaires, indépendamment des circonstances susceptibles d'engager leur responsabilité civile ou pénale.

La transmission d'informations confidentielles ne peut être réalisée qu'aux conditions suivantes :

- habilitation de l'émetteur ;
- désignation d'un destinataire autorisé ;
- respect de la procédure sécurisée interne prévue à cet effet.

La transmission de données à caractère personnel ne peut être réalisée qu'aux conditions suivantes :

- information du Responsable du traitement des données par l'Utilisateur ;
- Obtention préalable de l'autorisation de l'Autorité de Protection des Données à caractère Personnel en cas de transmission vers un État étranger non membre de la CEDEAO conformément aux dispositions du Code du numérique ;
- autorisation de l'Utilisateur aux fins de la transmission sollicitée dans le respect des procédures internes de transmission ;

La société se réserve la prérogative, à sa discrétion, de manière temporaire ou définitive, d'accorder, de refuser, de modifier ou de supprimer en tout ou partie, le droit d'accès de toute personne pour des raisons liées directement à la continuité et la sécurité des services.

12 Engagements de l'utilisateur

L'utilisateur s'engage en outre à :

- prévenir sans délai en cas de perte, vol ou faille de sécurité ;
- mettre en œuvre tous les moyens de sécurité prévus par les fonctionnalités des matériels et outils à sa disposition (smartphone, tablettes, ordinateurs, etc.) et qui sont demandés et notamment le code d'accès ;
- utiliser des codes d'accès (pin, verrouillage clavier et autre) différents et respectant le niveau de sécurité exigé par la présente ;
- se déconnecter de toutes applications après usage et ne pas rester connectés par défaut ;
- être vigilant vis à vis des données contenues dans les appareils à lui remis.

13 La cessation de l'utilisation

Lors de son départ de la société, l'utilisateur doit respecter la procédure de départ et remettre l'ensemble des moyens informatiques et de communication électronique qui lui ont été remis (ordinateur, périphériques, mobile, carte d'accès, moyen d'authentification à distance, badges, supports de stockage, etc.) en bon état général de fonctionnement et ne conserver aucun matériel ou aucune donnée permettant d'accéder au système d'information. De plus, l'utilisateur s'interdit, avant son départ, de détruire des informations et des données professionnelles. Il s'engage également à restituer, conformément aux procédures internes, les données à caractère personnel mises à sa disposition dans le cadre de son activité.

Sauf nécessité liée à la continuité du service et pour un temps raisonnable qui ne saurait excéder [**trois mois**], le compte messagerie de l'utilisateur est supprimé le jour de son départ. Toute, dès le date de la fin de son contrat, son accès lui est bloqué.

Dans le cas où le compte messagerie est toujours actif, même après le départ d'un utilisateur, une redirection des messages peut être mise en place par la société vers l'utilisateur ayant repris le poste de l'utilisateur ayant quitté la société ou toute autre personne occupant une fonction similaire.

14 Sécurité générale

14.1 Règles à respecter

Du fait de la collecte de données et du traitement de celles-ci, la société s'engage, dans le cadre des dispositions légales et réglementaires, à mettre en œuvre toutes les mesures organisationnelles et techniques utiles afin de préserver la sécurité, l'intégrité et la confidentialité des Données, ainsi que la sécurité de son système d'information et de communication, sur le plan technologique et procédural, afin notamment d'empêcher toute modification, tout transfert et toute suppression non-autorisés des Données, et toute intrusion non-autorisée dans son système d'information ou son endommagement.

Toutefois, le premier risque reste le risque humain lié aux traitements et aux manipulations des Données par les Utilisateurs, et par l'utilisation par ces derniers du système d'information et de communication et des outils qui y sont liés.

Par conséquent, la mise en place d'outils de sécurité ne doit pas dispenser les utilisateurs de signaler toute tentative d'intrusion extérieure, de falsification ou de présence de virus au responsable des systèmes d'information.

Tout utilisateur a la charge, à son niveau, de contribuer à la sécurité des moyens mis à sa disposition et du réseau auquel il a accès, principalement en évitant l'intrusion de virus susceptibles d'endommager le système d'information de la société.

14.2 Obligations de l'utilisateur

L'utilisateur s'oblige à :

- ne pas ouvrir les pièces jointes reçues de l'extérieur quand l'émetteur du message est inconnu ;
- détruire les messages du type « chaîne de solidarité » ;
- ne pas stocker et router des gadgets reçus ou trouvés sur internet ;
- ne pas faire suivre les messages d'alerte de l'arrivée d'un virus mais prévenir le responsable des systèmes d'information ;
- modifier la configuration de son poste de travail informatique effectuée par la direction des systèmes d'information, que ce soit par adjonction, suppression ou modification, sauf exception après accord exprès de cette dernière ;
- mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux à travers les matériels dont il a usage;
- utiliser (même avec leur accord) ou tenter d'utiliser des comptes autres que ceux qui lui sont attribués ou masquer son identité ;
- ne pas sortir les équipements informatiques de la société en dehors du site qui l'abrite, sauf accord du responsable du système d'information;
- ne pas télécharger de fichiers, en particulier médias, sans rapport avec l'activité professionnelle ou présentant un risque pour le système d'information ;

L'utilisateur est tenu d'informer sans délai sa hiérarchie de tout dysfonctionnement, altération, perte, vol, destruction et autre événement pouvant affecter les moyens informatiques et de communication électronique.

Toute installation ou utilisation de logiciels non expressément autorisées par le responsable des systèmes d'information est interdite.

Dans le cadre de ses déplacements professionnels, peu importe leur durée ou leur fréquence, l'utilisateur se doit d'adopter une attitude de prudence et de réserve au regard des informations et des ressources du système d'information auquel il pourrait être amené à accéder, manipuler ou échanger.

En particulier, il est déconseillé d'utiliser les systèmes de connexion wifi dans les lieux publics.

15 Exigences de reporting

Des rapports d'incidents quotidiens doivent être produits et traités par le service de sécurité informatique ou l'équipe d'intervention sur incident.
Des rapports d'incidents hebdomadaires détaillés doivent être produits par le service de sécurité informatique et envoyés au DSI.
Les incidents hautement prioritaires découverts par le service de sécurité informatique doivent être immédiatement remontés. Le DSI doit être contacté aussi vite que possible.
Le service de sécurité informatique doit également produire un rapport mensuel indiquant le nombre d'incidents de sécurité informatique et le pourcentage d'entre eux qui ont été résolus.

16 Informations complémentaires

L'utilisation des systèmes d'information implique le respect des droits de propriété intellectuelle de l'entreprise, de ses partenaires et, de tout tiers titulaire de tels droits. Dans le doute, l'utilisateur devra contacter le responsable des systèmes d'information qui s'en réfèrera, au besoin, à la Direction Marketing et Marque ou à la Direction juridique.

Chaque utilisateur autorisé s'engage à :

- utiliser les progiciels dans les conditions de la licence souscrite ;

- ne pas reproduire ou utiliser les progiciels, bases de données, page web ou autre création protégés par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation du titulaire de ces droits et en conformité avec le règlement en place dans le Service ;
- ne pas copier ou diffuser de textes, d'images, de photographies, d'œuvres musicales, audiovisuelles ou toute création copiée sur le réseau internet.

L'utilisateur est informé que la contrefaçon est un délit passible de sanctions civiles et pénales.

La présente charte est communiquée individuellement à chaque salarié par voie électronique.

Le Directeur des Systèmes d'Information peut fournir aux salariés /consultant/prestataires /utilisateurs toute information concernant l'utilisation du système d'information, en particulier sur les procédures de sauvegarde, de sécurité et sur les droits des Personnes Concernées.

Il les informe régulièrement sur l'évolution des limites techniques du système d'information et de communication ainsi que sur les menaces susceptibles de peser sur sa sécurité.

Chaque utilisateur doit se conformer aux procédures et règles de sécurité édictées par le Directeur des Systèmes d'Information dans le cadre de la présente charte.

Le DSI assurera la formation des Utilisateurs à leur entrée et de façon périodique à l'application des règles d'utilisation du système d'information et de communication prévues.

17 Autorité de Protection des Données à caractère Personnel

Les données à caractère personnel sont traitées par la société conformément aux conditions de Déclaration, Autorisation et de traitement prévues par la loi n°2017-20 du 20 avril 2020 portant Code du numérique en République du Bénin.

Les utilisateurs ont consenti à la collecte de leurs données à caractère personnel. Ils sont informés que les données à caractère personnel les concernant sont conservées par la société pendant toute la durée de leur relation contractuelle et des délais en matière de prescription.

Conformément à la loi, les utilisateurs sont informés qu'ils disposent de l'ensemble des droits prévus aux articles 437 et suivants de la loi 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin notamment les droits d'accès, d'interrogation, de portabilité, d'opposition, de rectification, de suppression, à l'oubli.

Les utilisateurs sont également informés que, pour des motifs légitimes, ils peuvent s'opposer au traitement des données personnelles les concernant.

La société informe ses collaborateurs et les salariés des entreprises adhérentes de leurs droits concernant leurs données personnelles à caractère particulier ou non, et doit aussi recueillir le consentement des collaborateurs comme des salariés.

18 Instances représentatives du personnel (IRP)

Toute utilisation des outils technologiques mis en place par la société pour ses utilisateurs est strictement et expressément interdite à des fins syndicales et/ou de revendications pour quelque cause que ce soit.

Les membres des IRP sont soumis aux autres dispositions de la présente charte.

Dans le cadre de leur mandat, les correspondances et informations échangées et stockées par les IRP sont, par principe, confidentielles et ne sont pas susceptibles d'être contrôlées, sauf lorsqu'un texte le prévoit.

19 Sanctions

Il est rappelé que la présente charte est un document à portée juridique, et donc contraignante pour les Utilisateurs.

En effet, les manquements aux règles et mesures de sécurité décrites dans la présente charte sont susceptibles d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés. Dans ce dernier cas, les procédures prévues dans le règlement intérieur et dans le Code du travail seront appliquées.

La société se réserve également le droit d'engager ou de faire engager des poursuites pénales et/ou civiles, indépendamment des sanctions disciplinaires mises en œuvre, notamment mais pas limitativement en cas de fraude informatique, de non-respect des droits d'auteur ou de violation du secret des correspondances.

Le responsable des systèmes d'information peut effacer ou isoler et conserver aux fins de preuve toute trace de logiciels, progiciels, programmes ou fichiers créés ou introduits dans le système d'information de la société, en violation des droits des tiers, notamment de propriété intellectuelle, et dénoncer tout acte délictueux aux autorités, sans préjudice de l'application de sanctions dans le cadre de son statut.

20 Entrée en vigueur et abrogation

La présente Politique a été adoptée par le Conseil d'Administration du REVELATEUR et est entrée en vigueur le jour de son adoption.
Elle abroge tout autre document ou texte adopté antérieurement portant sur les mêmes objets.