

L'identification numérique dans la gestion des ressources humaines

Amélioration de la sécurité,
efficacité et commodité, tout en
réduisant les risques et la fraude

Le point de vue d'Interac Corp.



« L'identification numérique deviendrait l'identifiant unique qui relie une personne à ses titres de compétences et à ses diplômes. »

Introduction

Afin de gérer efficacement les ressources humaines, un employeur doit analyser précisément l'ensemble des compétences qu'un employé potentiel prétend posséder. Toutefois, il est de plus en plus difficile de comprendre et de vérifier entièrement et efficacement ces compétences. De plus, les méthodes courantes utilisées pour sélectionner des candidats, déterminer leur compatibilité avec l'organisation et effectuer les vérifications avant l'embauche peuvent être extrêmement lentes et inefficaces. La possibilité de présenter des titres de compétences vérifiables permettrait aux employeurs de confirmer instantanément les qualifications d'un candidat.

Des titres de compétences vérifiables liés à des identifiants numériques uniques pourraient moderniser la gestion des ressources humaines, en particulier la relation entre les employés, les employeurs, les institutions reconnues et les gouvernements. L'identification numérique deviendrait l'identifiant unique qui relie une personne à ses titres de compétences et à ses diplômes.

Les employeurs pourraient facilement valider les titres de compétences d'un candidat, délivrés par des institutions reconnues,

tandis que les gouvernements pourraient demander des dossiers d'emploi pour accéder à des services publics et accomplir d'autres activités, comme la fiscalité. Plus important encore, les individus seraient en mesure d'accorder ou de retirer l'accès à leur curriculum vitæ validé, à leurs renseignements bancaires confidentiels et à d'autres données personnelles immuables, tout en les protégeant.

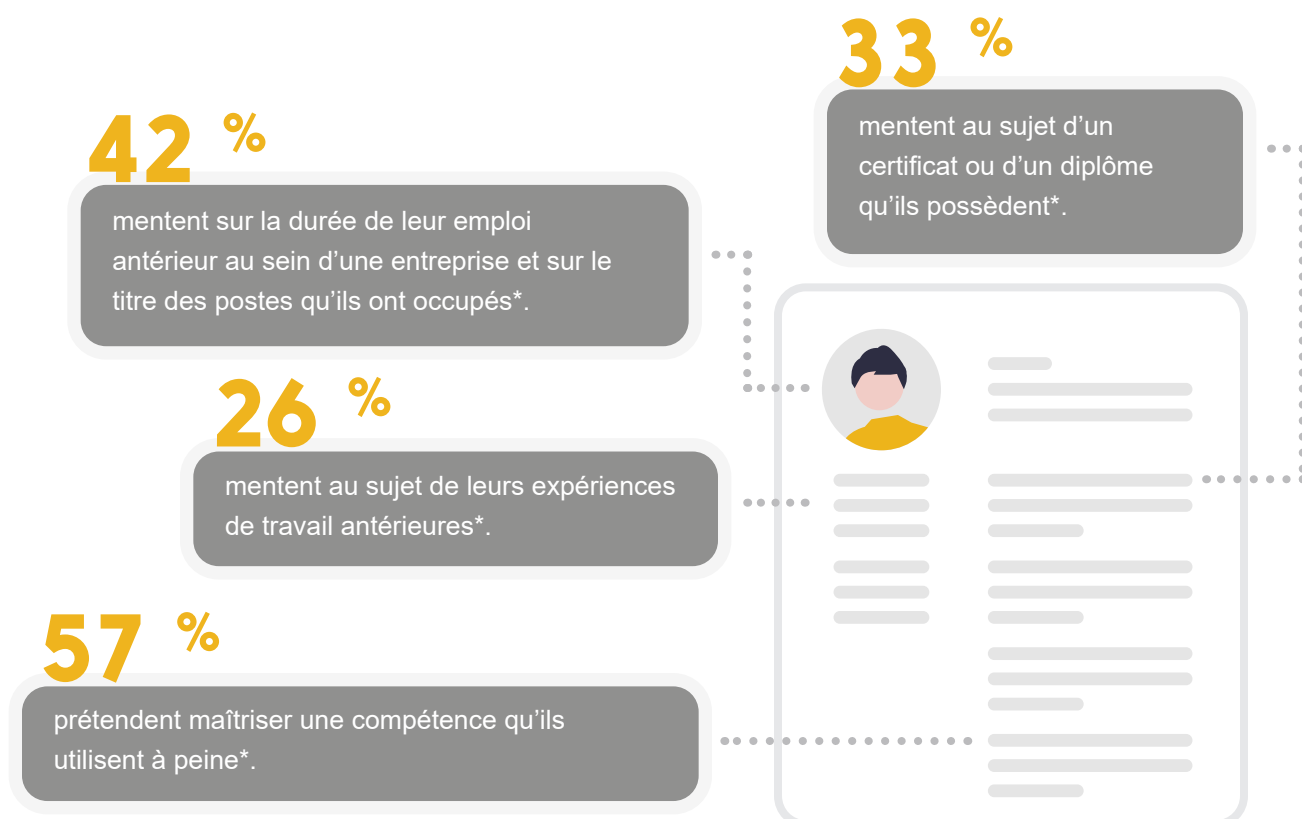
En plus de l'efficacité offerte par l'automatisation du recrutement, l'identification numérique améliorerait la surveillance en matière de sécurité, réduirait le risque de fraude, permettrait de valider les qualifications et réduirait les ressources nécessaires pour trouver et embaucher des talents dans l'économie moderne.



Comment les RH évolueront-elles au Canada?

Des sondages ont révélé que de nombreux candidats à un emploi font de fausses déclarations sur leur expérience de travail ou leurs études antérieures. La possibilité de vérifier les titres de compétences du demandeur, ceux-ci étant liés aux identifiants numériques émis par le gouvernement, non seulement atténuerait le risque de fraude, mais accroîtrait considérablement l'efficacité pour confirmer l'expérience de travail antérieure, les qualifications ou les diplômes universitaires du demandeur.

Pour demeurer concurrentiel dans une industrie moderne, numérique et axée sur les services, il faudra analyser et traiter un grand nombre de demandes afin de dénicher les meilleurs talents. Au-delà de la vérification des antécédents, l'identification numérique permettrait également aux employeurs de sécuriser les dossiers des employés, d'émettre des contrats intelligents, de se conformer aux règlements, et de gérer les paies et les avantages.



* Source des données présentées dans le graphique (en anglais seulement) :

[Career Builder \(2014\) Fifty-eight Percent of Employers Have Caught a Lie on a Resume. According to a New CareerBuilder Survey](#)

Comment l'identification numérique peut-elle aider?

Au-delà de l'amélioration de la sécurité, de l'efficacité et de la commodité, un réseau d'échange d'identification numérique permettrait également à toutes les parties impliquées d'échanger des données de manière conforme, ce qui fera progresser globalement l'attribution et la gestion du capital humain.

Employeurs

Renforce la sécurité en ne stockant pas les renseignements confidentiels des employés, mais en permettant plutôt aux demandeurs d'autoriser l'accès aux renseignements pertinents, au besoin, en utilisant un jeton.

Accroît la capacité et l'efficacité – tout en atténuant le risque de fraude liée aux compétences détenues – lors de la vérification des qualifications des candidats, comme l'expérience de travail, les titres de compétences ou les diplômes universitaires.

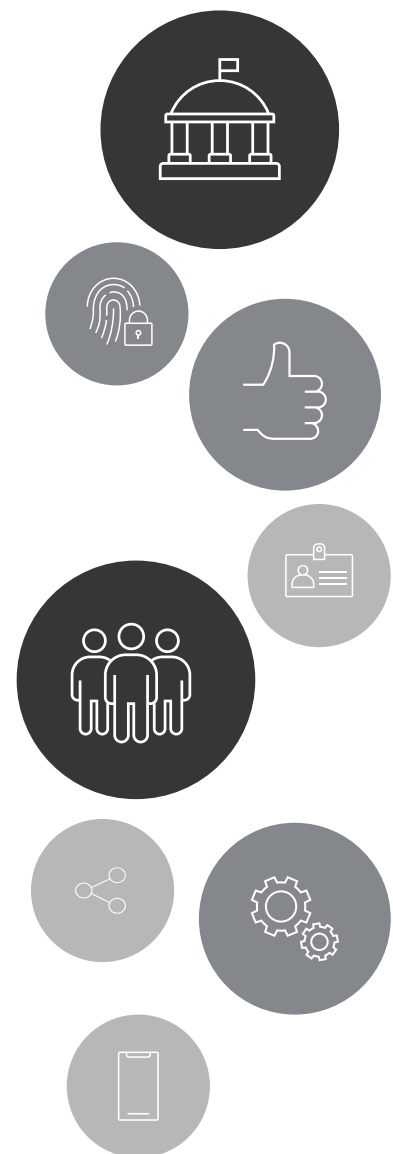
Réduit les coûts en augmentant la probabilité d'embaucher des talents qualifiés et la rétention du personnel.

Demandeurs

Offre une plus grande commodité en réduisant la quantité de documents échangés et la durée du processus d'entrevue.

Donne un aperçu détaillé des renseignements qu'un employeur demande et à quelles fins. C'est ce en quoi consiste le consentement éclairé, un élément essentiel de toute solution d'identification numérique.

Permet la conformité des données en permettant aux employés de retirer l'accès à un employeur aux renseignements personnels au moment de la cessation de l'emploi.



Parcours de l'utilisateur

L'identification numérique permettra de vérifier automatiquement les qualifications, d'éliminer la nécessité de stocker des données sensibles et d'améliorer radicalement le processus d'authentification et la sécurité par l'utilisation de jetons. Les avantages deviennent évidents à chaque étape du cycle d'un emploi.

Étape 1 :

Soumission du curriculum vitæ

Ivan souhaite poser sa candidature pour un poste de concepteur de produits dans une entreprise de technologie en croissance. Il est sur le point de soumettre sa candidature pour le poste, mais l'entreprise lui demande une preuve de diplôme de premier cycle avant d'aller de l'avant. Sur le site Web de l'entreprise, il est invité à vérifier numériquement son diplôme de premier cycle, émis par son université.

Étape 2 :

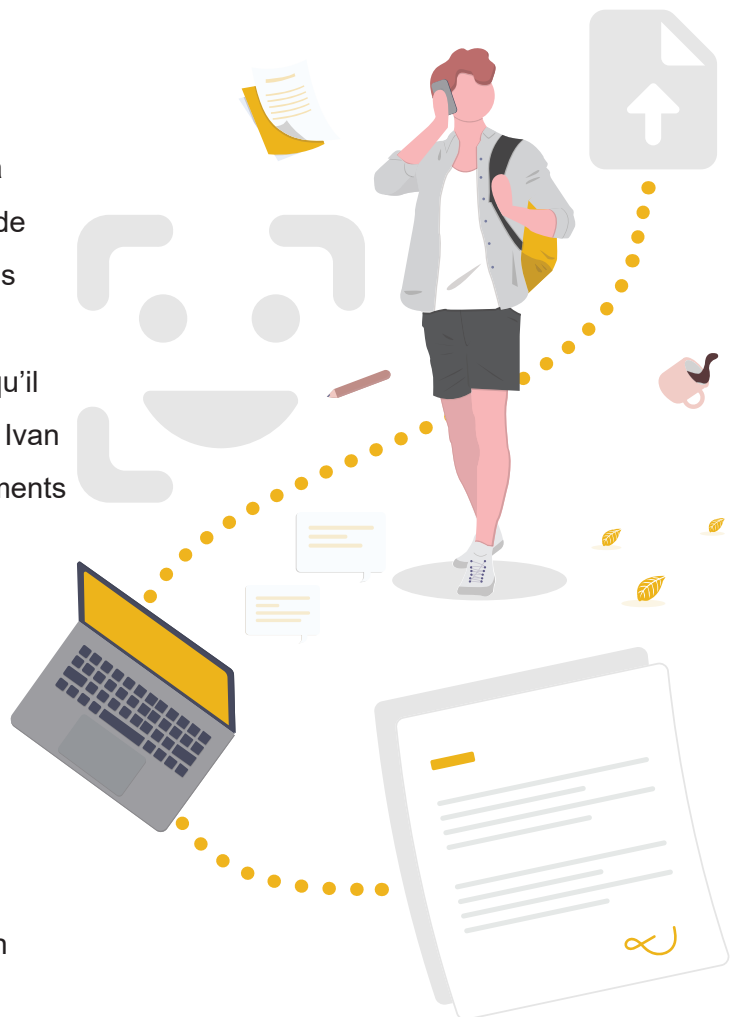
Participation à l'entrevue

Puisqu'il répond aux exigences du poste, il a été invité à une entrevue virtuelle. Au cours de l'entrevue, on lui pose des questions précises sur son expérience de travail antérieure. Le recruteur envoie à Ivan une demande pour qu'il partage les coordonnées de ses références. Ivan consent à accorder l'accès à ces renseignements supplémentaires.

Étape 3 :

Acceptation de l'offre

Au courant de la semaine, Ivan reçoit une offre qui contient la description de son nouveau poste, son salaire, la structure des primes et ses avantages sociaux. Ivan signe numériquement et est prêt à commencer son travail immédiatement.



Parcours de l'utilisateur (suite)

Étape 4 :

Réception du paiement

Lorsqu'il ouvre une session, Ivan est invité à partager son numéro d'assurance sociale et ses renseignements bancaires avec les RH. Il accepte. L'entreprise peut maintenant l'inscrire comme employé, et effectuer un dépôt direct chaque semaine.

Étape 5 :

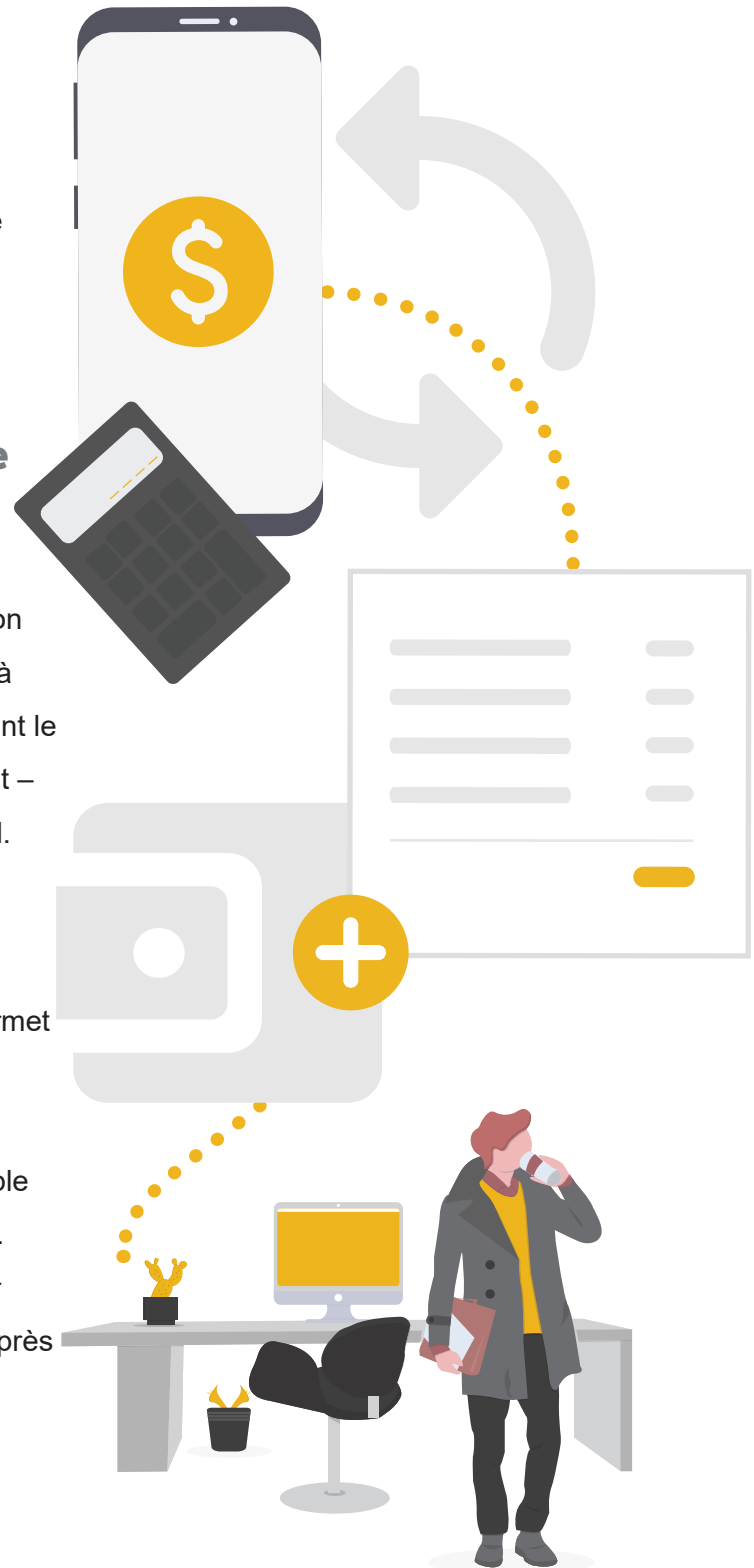
Soumission d'une déclaration de revenus

Ivan occupe ce poste depuis six mois, et la période des impôts approche à grands pas. Son employeur lui remet un feuillet T4, qu'il ajoute à son portefeuille numérique, pour éventuellement le partager – comme tout autre formulaire d'impôt – avec les gouvernements provinciaux et fédéral.

Étape 6 :

Cessation de l'emploi

Ivan a trouvé une nouvelle occasion qui lui permet de toucher un salaire plus élevé. Il a donné un préavis de deux semaines. Son employeur actuel lui remet un titre de compétence vérifiable qu'il pourra utiliser comme référence à l'avenir. Ivan peut retirer l'autorisation à son employeur d'accéder à ses renseignements personnels après sa dernière journée de travail.



Qu'est-ce qu'un titre de compétence vérifiable?

Un titre de compétence vérifiable est une preuve numérique d'attributs vérifiables, comme une qualification (diplôme universitaire) ou un renseignement (numéro d'assurance sociale). Il valide les qualités ou la propriété d'une affirmation faite par un utilisateur, en confirmant son existence et son caractère unique¹.

1. [W3C Working Group \(2019\) – \(en anglais seulement\)](#)

Nos principes

Il est facile de discuter de l'identification numérique de manière théorique, mais il est beaucoup plus complexe de concevoir une architecture et de mettre en œuvre un système d'identification numérique complet, sécuritaire et durable. Pour ce faire, il faut suivre un ensemble de principes clairement définis. Selon nous, cinq principes sont essentiels :



Contrôle par l'utilisateur et commodité

Personne ne veut confier ses renseignements personnels à un système si les données doivent être transférées et stockées par de nombreuses parties, surtout si cela se fait à l'insu de l'utilisateur et sans son consentement exprès. En plus de veiller au contrôle par l'utilisateur, un système d'identification doit être commode et facile à utiliser. Si ce n'est pas le cas, les gens, qui sont nombreux à être déjà habitués aux applications intuitives des appareils mobiles, ne voudront pas l'adopter.

Normes et ouverture

Dans un système dynamique, il est difficile de prédire l'avenir. Il est donc important d'établir des solutions qui sont conformes à des normes acceptées de façon universelle. Non seulement cela permet-il d'éliminer des dépenses liées à l'établissement du système de base et à l'adaptation de solutions ou à la création de solutions ponctuelles par la suite, mais cela permettra aussi de relier à la solution initiale des solutions créées par d'autres à l'avenir. L'ouverture favorise l'adoption, l'innovation et la souplesse.

Omniprésence

Lorsque les gens créent différents identifiants et mots de passe pour tous les services publics et privés auxquels ils doivent accéder, les menaces à la sécurité augmentent, car ils vont le plus souvent se limiter à un seul mot de

passer facile à mémoriser (et facile à deviner). De plus, un identifiant numérique ne donnant accès qu'à un nombre limité de services ne suscitera probablement pas une grande adhésion. Un système omniprésent sera donc plus commode et plus sécuritaire.

Marque de confiance

Aucun utilisateur n'est susceptible d'adopter une solution d'identification conçue ou maintenue par une organisation en laquelle il n'a pas confiance. La question de l'identité est trop importante et les répercussions du vol d'identité sont trop grandes pour s'en remettre au hasard. De plus, l'établissement d'une solution à grande échelle (et omniprésente) exige la coopération et la coordination de nombreux intervenants, et ces derniers doivent pouvoir se faire confiance, et avoir confiance en l'organisation dirigeant cette initiative.

Sécurité par l'abstraction

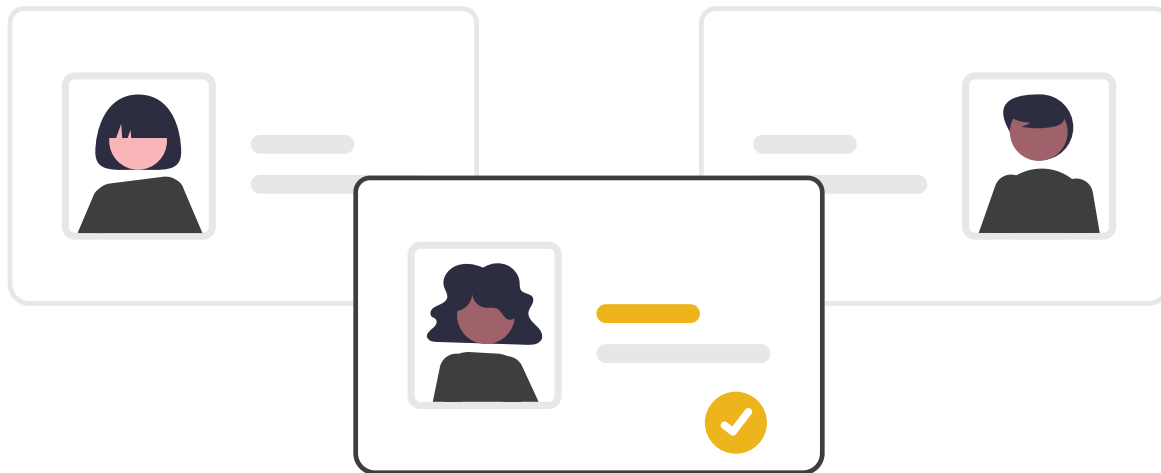
Même avec les meilleurs contrôles par l'utilisateur, certaines données d'identification doivent faire partie des transactions de tout écosystème. L'une des façons les plus efficaces de sécuriser ces données est de les rendre « abstraites » en remplaçant un identifiant privé par un identifiant public (comme l'adresse de courriel d'une personne), ou par un numéro aléatoire utilisé comme une sorte de jeton autorisé aux fins de l'opération, et utilisé à aucune autre fin.

Conclusion

Dénicher le bon talent pour un poste est un processus laborieux. Il consiste à passer en revue une pléthore de curriculum vitæ et de lettres de présentation, puis à consacrer un temps précieux à valider les affirmations et les qualifications d'un demandeur. Un cadre d'identification numérique normalisé s'intégrera à l'écosystème émergent des ressources humaines où l'identité et les compétences d'un utilisateur sont authentifiées de façon sécuritaire sans copier ni stocker de renseignements confidentiels.

Les employeurs ne seront pas responsables du stockage des renseignements des employés, car ceux-ci seront exclusivement détenus, partagés et retirés par l'employé. Par conséquent, l'identification numérique joue un rôle de premier plan dans le stockage, et le partage des compétences et des qualifications d'un utilisateur, en plus de ses renseignements personnels ou confidentiels.

À mesure qu'un plus grand nombre d'institutions agréées et de plateformes d'éducation reconnues commenceront à émettre des titres de compétences vérifiables, les entreprises tireront sans aucun doute parti de cette approche qui demande peu de ressources pour analyser les candidatures et trouver la bonne personne pour un poste.



Si vous souhaitez collaborer avec *Interac* au sujet de l'avenir de l'identification numérique, écrivez-nous à :

digitalid@interac.ca

« Un cadre d'identification numérique normalisé s'intégrera à l'écosystème émergent des ressources humaines où l'identité et les compétences d'un utilisateur sont authentifiées de façon sécuritaire sans copier ni stocker de données sensibles. »



**Pour en savoir plus sur ce sujet,
visitez le site innovation.interac.ca.**

Publication : octobre 2021

Copyright © Interac Corp., 2021. Tous droits réservés.

Le logo Interac est une marque d'Interac Corp.

Sauf dans la mesure permise par la loi, le présent document ne peut être reproduit ou transmis, en tout ou en partie, sous quelque forme ou par quelque moyen que ce soit, électronique ou mécanique, y compris la photocopie, sans le consentement autorisé d'Interac Corp. Le présent document est fourni à titre indicatif uniquement, et Interac Corp., en le publiant, ne garantit aucunement que les renseignements qu'il contient sont ou resteront exacts. Interac Corp., y compris ses agents, ses dirigeants, ses actionnaires et ses employés, ne peut être tenue responsable envers toute partie de toute perte ou de tout dommage, quels qu'ils soient, se basant sur l'hypothèse de la fiabilité de l'information contenue dans le présent document.