Livre blanc de Tellent
Sécurité, conformité et exploitation

Avec ce document, Tellent vous fournit transparence et clarté sur ses politiques de sécurité, de conformité et d'exploitation qui constituent les fondements de nos activités et de nos partenariats. Parce que nous savons que faire appel à un fournisseur de services est une décision commerciale importante et que, comme tout partenariat, elle doit reposer sur la confiance.

Dans ce document, vous trouverez un aperçu général des mesures de sécurité prises par Tellent en tant qu'entreprise et dans les produits/modules SaaS des logiciels Tellent :

- KiwiHR by Tellent, un système de ressources humaines de base ;
- Javelo by Tellent, un système de gestion des performances ;
- Recruitee by Tellent, un système de suivi des candidats ;
- Tout autre service offrant des fonctionnalités unifiées entre les produits/modules susmentionnés.

Pour toute question, veuillez contacter Tellent via le chat d'assistance intégré dans l'application ou l'équipe de sécurité directement via : security@tellent.com

tellent

Table des matières

tellent

Rapports de conformité, de certification et d'audit

Certification ISO 27001 et rapport d'assurance SOC 2

Tellent :

- ISO 27001:2022
  - Un exemplaire de la certification ISO 27001 de Tellent est disponible ici.
  - La déclaration d'applicabilité ISO 27001 de Tellent est disponible ici.
  - Portée du certificat ISO 27001 de Tellent : *le développement, l'exploitation et la livraison sécurisés des produits/modules SaaS des logiciels Tellent suivants : système d'information sur les ressources humaines de base (également commercialisé sous la marque « KiwiHR »), gestion des performances (également commercialisé sous la marque « Javelo »), système de suivi des candidats (également commercialisé sous la marque « Recruitee ») et tout produit/module offrant des fonctionnalités unifiées entre ces produits/modules.*

SaaS Recruitee :

- SOC 2
  - Un exemplaire du rapport SOC 2 de Recruitee (SSAE 16/ISAE 3402 Type II) peut être fourni sur demande.

Audit interne et tests d'intrusion

- Le responsable de la sécurité de l'information (ISO) de Tellent, en collaboration avec divers auditeurs tiers spécialisés, vérifie la sécurité des services et des processus de l'entreprise.
- Des tests d'intrusion sont effectués régulièrement par des entreprises de sécurité réputées.
- Les clients peuvent effectuer leurs propres tests d'intrusion et audits sur demande.

RGPD

- Tellent facilite votre capacité à vous conformer au RGPD, y compris en offrant des fonctionnalités RGPD dédiées.
  - Nos responsables de la réussite client et notre équipe d'assistance dédiés sont en mesure d'aider à la configuration et de répondre à toutes les questions relatives aux fonctionnalités.
- Notre addendum normalisé sur le traitement des données (DPA) fait partie de l'accord entre Tellent et vous en tant que client, sauf accord contraire explicite.
- La conformité au RGPD de Tellent est surveillée par le service juridique interne de Tellent.
- Toutes les données personnelles traitées pour le compte de nos clients sont stockées au sein de l'Union européenne et ne seront pas transférées vers des pays tiers sans votre accord.

- Tellent ne se conforme aux demandes gouvernementales d'accès aux données (personnelles) que dans la mesure où il est légalement tenu de le faire en vertu des lois et réglementations applicables.

Données client (y compris les données personnelles du client)

- Les données client sont toutes les données, y compris les données personnelles, traitées par Tellent pour le compte d'un client dans le cadre du SaaS, à l'exclusion des sauvegardes.
- En ce qui concerne les données personnelles des clients en particulier, les clients sont considérés comme le responsable du traitement de ces données personnelles et Tellent le sous-traitant des données, tel que défini plus en détail dans notre addendum sur le traitement des données (DPA).
- Tellent ne vend, ne fait de la publicité ou n'utilise jamais les données des clients d'une autre manière que pour fournir ou améliorer les services fournis à ses clients.
- Les clients peuvent exporter les données client en utilisant les API de Tellent ou toutes les fonctionnalités d'exportation disponibles dans le cadre du SaaS.

Sécurité des applications

Accès basé sur l'identité et le rôle

Le statut ou l'accès aux rôles et aux autorisations des membres peut être défini dans le centre d'administration Tellent et/ou individuellement via les SaaS Recruitee, Javelo ou KiwiHR.

Grâce à ces différents réglages, il est (par exemple) possible de :

- dans le SaaS Recruitee, limiter les informations sur les postes vacants aux gestionnaires d'embauche uniquement ;
- dans le SaaS Javelo, afficher uniquement l'état ou les résultats des enquêtes ou des campagnes ouvertes aux employés qui font partie de votre équipe RH ;
- dans le SaaS KiwiHR, autoriser que les données et les détails d'un employé ne soit montrés qu'à son responsable direct ;
- à partir du SaaS Recruitee, partager les données des candidats avec les non-utilisateurs à l'aide de liens uniques ;
- dans le SaaS Recruitee, appliquer des fonctionnalités de visibilité aux champs de profil des candidats qui ont postulé, par exemple, pour empêcher les indications de salaire d'être visibles.

L'article d'assistance contenant plus d'informations sur la gestion des paramètres du compte sur le **centre d'administration Tellent** est disponible sur :
https://support.tellent.com/en/collections/9447061-account-settings

L'article d'assistance contenant plus d'informations sur la gestion des paramètres du compte dans le **SaaS Javelo** est disponible sur :
https://support.javelo.com/en/collections/9545584-account-settings

L'article d'assistance contenant plus d'informations sur la gestion des rôles d'utilisateur dans le **SaaS KiwiHR** est disponible sur :
https://support.kiwihr.com/en/articles/9345339-user-roles et
https://support.kiwihr.com/en/articles/9345338-access-levels

L'article d'assistance contenant plus d'informations sur les rôles d'utilisateur (rôles d'embauche) dans le **SaaS Recruitee** est disponible sur :
https://support.recruitee.com/en/articles/1066251-hiring-roles

Sécurité des données en transit et chiffrement

- Toutes les données sont transférées sur Internet à l'aide de TLS 1.2 ou supérieur avec une taille de clé publique de 2 048 bits minimum.
- Les cookies contenant des informations sensibles sont définis comme « sécurisés » et « HTTP uniquement ».
- Les données client sont chiffrées au repos (AES 256 ou supérieur).

Codage sécurisé

- Les efforts des développeurs visent à atténuer les 10 principaux risques de l'OWASP et à suivre les meilleures pratiques du secteur en matière de sécurité.
- Des tests automatisés sont configurés pour vérifier automatiquement que l'application fonctionne comme il se doit.
- L'automatisation a été configurée pour vérifier automatiquement les vulnérabilités dans le code et les dépendances.
- Le nouveau code est testé par l'équipe d'assurance qualité de Tellent.
- Les données de production ne sont jamais utilisées pour les tests. Tellent dispose d'un (de plusieurs) environnement(s) de mise en scène distinct(s).
- Tout le code est soumis à un examen.

Protection contre les logiciels malveillants et les scripts intersites

- Les chargements de fichiers par les candidats et les utilisateurs finaux sont analysés à la recherche de logiciels malveillants. Les définitions sont mises à jour automatiquement et régulièrement.
- Les données des champs de saisie utilisateur sont nettoyées.
- Les développeurs suivent les meilleures pratiques, telles qu'atténuer les 10 principaux risques de l'OWASP, empêcher les scripts intersites (XSS), l'injection SQL (SQLi) et la falsification de demandes intersites (CSRF).

Authentification

- Il est possible d'intégrer votre propre fournisseur d'identité Single Sign On (via SAML 2.0).

    - Pour les comptes sans SSO, les connexions sont basées sur l'adresse e-mail et le mot de passe de l'utilisateur final.
    - Les nouveaux mots de passe doivent comporter au moins 8 caractères, y compris chacun des types de caractères suivants : lettre majuscule, lettre minuscule et chiffre.
- Une fois authentifié avec succès, un jeton d'accès est accordé.
    - Chaque appareil de l'utilisateur final reçoit un jeton d'accès unique.
    - Les jetons sont stockés en toute sécurité (cookies, « sécurisés » et « HTTP uniquement »).
- Tous les jetons d'accès sont révoqués lorsqu'un utilisateur modifie son mot de passe. Cela inclut les changements de mot de passe via la fonctionnalité « mot de passe oublié ».
- Les jetons d'accès expirent après 30 jours et sont révoqués après la déconnexion d'un utilisateur final. Les anciens jetons d'accès sont régulièrement remplacés par des nouveaux pendant l'utilisation continue de l'application.
- Tellent stocke uniquement les hachages des mots de passe pour les comptes d'utilisateurs, et non les mots de passe eux-mêmes. Les hachages sont générés à l'aide d'un algorithme standard du secteur et selon les meilleures pratiques.
- Après un nombre élevé de tentatives de connexion sur un compte, il sera temporairement bloqué.

Protection des e-mails

- Les serveurs de messagerie sortants et entrants de Tellent prennent en charge TLS.
- SPF, DMARC et DKIM sont utilisés pour tous les e-mails sortants.
- Le client peut entièrement contrôler la sécurité de l'intégration de l'e-mail en connectant le SaaS Recruitee à son propre serveur IMAP et SMTP via TLS. Cela permettrait également au client de bénéficier de SPF, DKIM et DMARC.
- Le SaaS Recruitee dispose également d'une fonctionnalité permettant de partager des candidats avec des non-utilisateurs via HTTPS au lieu de protocoles de messagerie moins sécurisés.

Hébergement, infrastructures techniques et physiques

Protection des serveurs et des infrastructures

- Un nombre minimal d'adresses IP publiques est utilisé. Seuls les serveurs frontaux ont des adresses IP publiques.
- Des pare-feu sont en place. La mise en œuvre est régie par une politique.
- L'infrastructure Google Cloud Platform et Amazon Web Services atténue et absorbe toutes les attaques (D)DOS des couches 4 et inférieures.
- Des processus automatisés et manuels ont été configurés pour analyser et détecter les vulnérabilités dans les logiciels de serveur et pour mettre à jour régulièrement ces logiciels.

tellent

Multi-tenant

- L'offre SaaS de Tellent est fournie dans un environnement multi-tenant qui est logiquement séparé. Cela offre une économie d'échelle et signifie que Tellent peut investir davantage dans des mesures pour protéger votre compte contre les pics de trafic.
- Les séparations logiques sont testées par l'équipe d'assurance qualité de Tellent et lors d'un test de pénétration tiers.
- À ce stade, Tellent n'offre pas de solutions single-tenant.

Journalisation et suivi

- De nombreuses activités des utilisateurs finaux peuvent être suivies dans le produit.
- Chaque appel API est enregistré. Les applications Tellent sont entièrement basées sur des interactions avec API.
    - Les applications Tellent offrent une fonctionnalité de journaux d'audit qui permet aux administrateurs d'afficher les journaux d'un grand nombre d'événements dans l'application.
    - Pour le SaaS Recruitee :
        - Une liste des événements enregistrés est disponible sur la page suivante :
            - https://docs.recruitee.com/docs/audit-logs
        - Des informations plus générales sur la fonctionnalité des journaux d'audit sont disponibles ici :
            - https://support.recruitee.com/en/articles/5661032-audit-logs
    - Pour le SaaS KiwiHR :
        - Des instructions sur la façon d'afficher un journal des modifications apportées à la saisie de données du profil de l'employé sont expliquées plus en détail ici :
            - https://support.kiwihr.com/en/articles/9345331-kiwihr-plus-features#h_624211bc16
    - Pour le SaaS Javelo :
        - Il est possible de suivre les progrès de la campagne. Des instructions sur la façon d'afficher les rapports sont disponibles ici :
            - https://support.javelo.com/en/articles/9345449-how-to-access-the-detailed-page-of-a-campaign
            - https://support.javelo.com/en/articles/9345600-how-does-the-my-team-tab-work
    - Veuillez noter que tous les journaux ne sont pas disponibles via la fonctionnalité des journaux d'audit. Des journaux détaillés sont disponibles sur demande.
- L'accès des employés de Tellent aux comptes appartenant aux clients est enregistré. Les employés ne sont généralement autorisés à accéder aux comptes qu'après avoir reçu le consentement de l'utilisateur final.

- Les applications Tellent sont automatiquement surveillées et les interruptions sont suivies 24 h/24 et 7 j/7 par les ingénieurs de Tellent.
    - L'état des applications Tellent peut être surveillé via https://status.tellent.com
- Des tests automatisés sont configurés par l'équipe d'assurance qualité pour vérifier automatiquement que l'application fonctionne comme il se doit.
- L'accès aux serveurs sous la gestion ou le contrôle de Tellent est enregistré.
- Des systèmes de détection d'intrusion sont en place.

Reprise après sinistre, sauvegarde et redondance

- Une politique de sauvegarde et de récupération est en place chez Tellent.
- Les serveurs Web sont configurés de manière redondante et évoluent automatiquement.
- L'hébergement de fichiers est configuré de manière extrêmement évolutive à l'aide d'Amazon S3.
- Des sauvegardes chiffrées de toutes les données appartenant aux clientssont effectuées au moins tous les jours et supprimées lorsqu'elles ne sont plus raisonnablement nécessaires.
- Les sauvegardes sont stockées dans différents centres de données.
- Tous les centres de données utilisés par Tellent disposent d'un plan de reprise après sinistre.

Fournisseurs d'hébergement et centres de données

- Tellent utilise Google Cloud Platform et Amazon Web Services pour héberger les applications Tellent.
- Les services fournis par Google Cloud Platform et Amazon Web Services à Tellent sont certifiés ISO 27001 et CSA STAR, et conformes SOC 2 (SSAE 16/ISAE 3402 Type II).
- D'autres sous-traitants ou fournisseurs d'hébergement sont également certifiés ISO 27001 et/ou conformes SOC 2 (SSAE 16/ISAE 3402 Type I).
    - Des détails supplémentaires figurent dans notre DPA.
- Des contrôles physiques solides sont en place dans tous les centres de données.
- Toutes les données hébergées dans ces centres sont supprimées de manière professionnelle après la mise hors service du matériel.

Bureaux

- Les bureaux sont sécurisés à l'aide d'un ensemble de caméras, d'alarmes, de gardes de sécurité et/ou de cartes-clés/keytags.
- Tous les ordinateurs portables des employés sont gérés par l'entreprise (MDM) et ont été protégés contre l'accès aux données par des personnes non autorisées.

Organisation et gestion, politiques et processus de sécurité

- Les employés de Tellent sont tenus de verrouiller leurs écrans lorsqu'ils s'en éloignent.
- Tellent s'efforce d'avoir un bureau sans papier.

- Tous les employés de Tellent sont tenus d'accepter les conditions de confidentialité (notamment, au moyen d'une END).
- Les employés de Tellent sont tenus d'utiliser exclusivement des mots de passe forts.
- Les appareils des employés de Tellent disposent d'un logiciel antivirus et sont chiffrés.
- Des politiques de contrôle d'accès sont en place pour s'assurer que l'accès est révoqué lorsque des employés ne font plus partie de Tellent. Le principe du moindre privilège est appliqué et activement surveillé.
- La sensibilisation à la sécurité est activement cultivée au sein de Tellent au travers d'une formation régulière.

Réponse aux incidents

- Un plan de réponse aux incidents de sécurité (SIRP) est en place chez Tellent.
- Le SIRP contient une désignation claire de l'autorité, les mesures à prendre en cas d'incident et une liste des membres internes et externes de l'équipe d'intervention.
- Le SIRP couvre également les réponses aux violations de données telles que requises en vertu du RGPD.
- Des exercices d'incident (sur table) sont effectués régulièrement avec les parties prenantes concernées.

Niveau de service et assistance

- Tellent vise une disponibilité de 99,5 % hors maintenance. Le bilan de Tellent est disponible ici : https://status.tellent.com
- L'équipe d'assistance de Tellent est disponible entre 9 h et 18 h (CET et EST), par e-mail et par chat en direct.
- Nos articles d'assistance sur https://support.tellent.com fournissent des conseils sur chaque mise à jour.
- Les modifications importantes apportées aux produits sont communiquées par e-mail et/ou via le service de chat intégré à l'application par notre équipe d'assistance clientèle.
- Les feuilles de route des produits sont disponibles sur : https://support.tellent.com/en/articles/9805760-tellent-hr-platform-roadmap-2024

Définitions

- Utilisateurs finaux : tous les utilisateurs, à l'exception des visiteurs du site Carrières, des candidats et des parrains.

Avertissement : ce document est destiné à donner au lecteur un aperçu général des mesures de sécurité, de conformité et d'exploitation prises par Tellent en relation avec le(s) service(s) à la date de « dernière mise à jour ». Certaines distinctions ou nuances peuvent être négligées. Veuillez contacter Tellent pour obtenir des informations plus spécifiques et/ou à jour.