Tellent Whitepaper
Beveiliging, Naleving en Operaties

Met dit document biedt Tellent u transparantie en duidelijkheid over zijn beleid op het gebied van beveiliging, naleving en operaties, die de basis vormen van onze bedrijfsvoering en samenwerkingen. Omdat we begrijpen dat het inschakelen van een serviceprovider een belangrijke zakelijke beslissing is en, net als elke samenwerking, gebaseerd moet zijn op vertrouwen.

In dit document vindt u een algemeen overzicht van de beveiligingsmaatregelen die Tellent als organisatie heeft genomen en in de Tellent Software-as-a-Service-producten/modules:

- KiwiHR van Tellent, een essentieel systeem voor human resources management
- Javelo van Tellent, een prestatiemanagementsysteem
- Recruitee van Tellent, een kandidaatvolgsysteem
- Elke andere dienst die een geïntegreerde functionaliteit biedt tussen de hierboven genoemde producten/modules.

Voor vragen kunt u contact opnemen met Tellent via de in-app ondersteuningschat of rechtstreeks met het beveiligingsteam via: security@tellent.com

tellent

Inhoud

tellent

Naleving, certificeringen en auditrapporten

ISO 27001-certificering en SOC 2-controlerapport

Tellent:

- ISO 27001:2022
  - Een kopie van Tellent's ISO 27001-certificering is hier te vinden.
  - Tellent's ISO 27001-verklaring van toepasselijkheid vindt u hier.
  - Omvang van Tellent's ISO 27001-certificaat: *De veilige ontwikkeling, werking en levering van de volgende Tellent Software as a Service-producten/modules: een essentieel systeem voor human resources management ook op de markt gebracht onder de merknaam "KiwiHR"), een prestatiemanagementsysteem (ook op de markt gebracht onder de merknaam "Javelo"), een kandidaatvolgsysteem (ook op de markt gebracht onder de merknaam "Recruitee") en elk product/module die geïntegreerde functionaliteit biedt tussen deze producten/modules.*

Recruitee SaaS:

- SOC 2
  - Een kopie van het SOC 2-rapport (SSAE 16/ISAE 3402 Type II) van Recruitee kan op verzoek worden verstrekt.

Interne audits en penetratietests

- Tellent's Information Security Officer (ISO), samen met verschillende gespecialiseerde externe auditors, voert controles uit op de beveiliging van de diensten en bedrijfsprocessen.
- Penetratietests worden regelmatig uitgevoerd door gerenommeerde beveiligingsbedrijven.
- Klanten kunnen op verzoek hun eigen penetratietests en -audits uitvoeren.

AVG

- Tellent maakt het mogelijk voor u om te voldoen aan de AVG, onder andere door het aanbieden van specifieke AVG-functies.
  - Onze toegewijde Customer Success managers en ons supportteam kunnen u helpen bij de configuratie en eventuele vragen over functies beantwoorden.
- Onze standaard Gegevensverwerkingsaddendum (DPA) maakt deel uit van de overeenkomst tussen Tellent en u als klant, tenzij uitdrukkelijk anders is overeengekomen.
- De naleving van de AVG door Tellent wordt gecontroleerd door de interne juridische afdeling van Tellent.
- Alle persoonlijke gegevens die namens onze klanten worden verwerkt, worden opgeslagen binnen de Europese Unie en mogen niet zonder uw toestemming aan derde landen worden overgedragen.

- Tellent voldoet alleen aan overheidsverzoeken om toegang te krijgen tot (persoonlijke) gegevens voor zover dit wettelijk vereist is op basis van de toepasselijke wetten en regelgeving.

Klantgegevens (inclusief persoonsgegevens van klanten)

- Klantgegevens zijn alle gegevens, inclusief persoonsgegevens, die door Tellent namens een klant worden verwerkt als onderdeel van de SaaS producten/modules, met uitzondering van back-ups.
- Met betrekking tot persoonlijke gegevens van klanten, worden klanten beschouwd als de gegevensbeheerder van deze gegevens en Tellent als de verwerker, zoals verder gedefinieerd in onze Gegevensverwerkingsaddendum (DPA).
- Tellent verkoopt, adverteert of gebruikt klantgegevens nooit op een andere manier dan voor het uitvoeren of verbeteren van de diensten die aan de klanten worden geleverd.
- Klanten kunnen klantgegevens exporteren door gebruik te maken van de API's van Tellent of andere exportfuncties die beschikbaar worden gesteld als onderdeel van de SaaS producten/modules.

Applicatiebeveiliging

Op identiteit en rol gebaseerde toegang

De status van, of toegang tot, rollen en machtigingen van leden kan worden ingesteld binnen het Tellent Admin Center en/of individueel via de Recruitee SaaS, Javelo SaaS of KiwiHR SaaS.

Via deze verschillende instellingen is het (bijvoorbeeld) mogelijk om:

- In de Recruitee SaaS wordt de informatie over openstaande vacatures beperkt tot alleen de wervingsmanagers.
- In Javelo SaaS wordt de status of de resultaten van open enquêtes of campagnes alleen weergegeven aan medewerkers die deel uitmaken van je HR-team.
- In KiwiHR SaaS wordt alleen de data en de details van een medewerker weergegeven aan hun directe manager;
- Vanuit Recruitee SaaS kunt u kandidaatgegevens delen met niet-gebruikers door middel van unieke koppelingen;
- In Recruitee SaaS worden zichtbaarheidfuncties toegepast op profielvelden van kandidaten die hebben gesolliciteerd, bijvoorbeeld om salarisindicaties te beschermen tegen zichtbaarheid.

Het ondersteuningsartikel met meer informatie over het beheren van accountinstellingen in het **Tellent Admin Center** is te vinden op:
https://support.tellent.com/en/collections/9447061-account-settings

Het ondersteuningsartikel met meer informatie over het beheren van accountinstellingen in **Javelo SaaS** is te vinden op:
https://support.javelo.com/en/collections/9545584-account-settings

Het ondersteuningsartikel met meer informatie over het beheren van gebruikersrollen in **KiwiHR SaaS** is te vinden op: https://support.kiwihr.com/en/articles/9345339-user-roles & https://support.kiwihr.com/en/articles/9345338-access-levels

Het ondersteuningsartikel met meer informatie over gebruikersrollen (wervingsrollen) in **Recruitee SaaS** is te vinden op: https://support.recruitee.com/en/articles/1066251-hiring-roles

Beveiliging van gegevens tijdens verzending en versleuteling

- Alle gegevens worden via internet overgedragen met behulp van TLS 1.2 of hoger met een openbare sleutelgrootte van minimaal 2048 bits .
- Cookies met gevoelige informatie worden ingesteld op "secure" en "http-only".
- Klantgegevens worden in rust versleuteld (AES 256 of beter).

Veilig codering

- De inspanningen van ontwikkelaars zijn gericht op het beperken van de OWASP Top 10-risico's en het volgen van de best practices voor beveiliging in de branche.
- Geautomatiseerde tests worden opgezet om automatisch te controleren of de applicatie naar behoren functioneert.
- Automatisering is ingesteld om automatisch te controleren op kwetsbaarheden in de code en afhankelijkheden.
- Nieuwe code wordt getest door het kwaliteitszorgteam van Tellent.
- Productiegegevens worden nooit gebruikt voor tests. Tellent beschikt over aparte stagingomgevingen.
- Alle code wordt onderworpen aan codebeoordeling.

Bescherming tegen malware en cross-site-scripting

- Bestanden die door kandidaten en eindgebruikers worden geüpload, worden gescand op malware. Definities worden regelmatig en automatisch bijgewerkt.
- Gegevens uit invoervelden van gebruikers worden geschoond.
- Ontwikkelaars volgen best practices, zoals de OWASP Top 10, om Cross Site Scripting (XSS), SQL-injectie (SQLi) en Cross Site Request Forgery (CSRF) te voorkomen.

Authenticatie

- Het is mogelijk om uw eigen Single Sign On-identiteitsprovider te integreren (via SAML 2.0)
    - Voor accounts zonder SSO zijn logins gebaseerd op het e-mailadres en wachtwoord van de eindgebruiker.
    - Nieuwe wachtwoorden moeten minimaal 8 tekens bevatten, inclusief elk van de volgende soorten tekens: een hoofdletter, een kleine letter en een cijfer.
- Na succesvolle verificatie wordt een toegangstoken toegekend.
    - Elk apparaat van de eindgebruiker krijgt een ander, individueel toegangstoken.

    - Tokens worden veilig opgeslagen (cookies, "secure" en "http-only")
- Alle toegangstokens worden ingetrokken wanneer een gebruiker zijn wachtwoord wijzigt. Dit omvat wachtwoordwijzigingen via de "wachtwoord vergeten"-functionaliteit.
- Toegangstokens verlopen na 30 dagen en worden ingetrokken nadat een eindgebruiker zich afmeldt. Oude toegangstokens worden regelmatig vervangen door nieuwe toegangstokens tijdens het voortdurende gebruik van de app.
- Tellent slaat alleen hashes van wachtwoorden op voor gebruikersaccounts, niet de wachtwoorden zelf. Hashes worden gegenereerd met behulp van een sterk standaardalgoritme en volgens de best practices.
- Na een groot aantal inlogpogingen op één account wordt deze tijdelijk geblokkeerd.

E-mailbeveiliging

- De uitgaande en inkomende e-mailservers van Tellent ondersteunen TLS.
- SPF, DMARC en DKIM worden gebruikt voor alle uitgaande mail.
- De klant kan de beveiliging van de e-mailintegratie volledig beheren door de Recruitee SaaS via TLS te verbinden met zijn eigen IMAP- en SMTP-server. Dat zou de klant ook in staat stellen om te profiteren van SPF, DKIM en DMARC.
- Recruitee SaaS heeft ook functionaliteit om kandidaten te delen met niet-gebruikers via HTTPS in plaats van minder veilige e-mailprotocollen.

Hosting, technische en fysieke infrastructuur

Bescherming van servers en infrastructuur

- Er wordt een minimale hoeveelheid openbare IP-adressen gebruikt. Alleen front-end servers hebben openbare IP-adressen.
- Firewalls zijn aanwezig. De implementatie wordt gedekt door een beleid.
- De infrastructuur van Google Cloud Platform en Amazon Web Services vermindert en absorbeert alle Layer 4 en lagere (D)DOS-aanvallen.
- Geautomatiseerde en handmatige processen zijn ingesteld om kwetsbaarheden in serversoftwarepakketten te scannen en te detecteren en om dergelijke pakketten regelmatig bij te werken.

Meervoudig gebruik

- Tellent's SaaS-aanbod wordt geleverd in een meervoudige gebruikers omgeving die logisch gescheiden is. Dit biedt schaalvoordelen en betekent dat Tellent veel kan investeren in maatregelen om uw account te beschermen tegen pieken in het verkeer.
- De logische scheidingen worden getest door het kwaliteitszorgteam van Tellent en tijdens een penetratietest van derden.
- Op dit moment biedt Tellent geen oplossingen voor een enkele huurder aan.

tellent

Logging en monitoring

- Veel activiteiten van eindgebruikers kunnen in het product worden gevolgd.
- Elke API-aanroep wordt geregistreerd. De Tellent-applicaties zijn volledig gebaseerd op interacties met de API('s).
    - De Tellent-applicaties bieden een functie voor auditlogs waarmee beheerders logs kunnen bekijken van een groot aantal gebeurtenissen in de applicatie.
    - Voor Recruitee SaaS:
        - Een lijst met de gebeurtenissen die worden geregistreerd, is beschikbaar op de volgende pagina:
            - https://docs.recruitee.com/docs/audit-logs.
        - Meer algemene informatie over de functie auditlogs vindt u hier:
            - https://support.recruitee.com/en/articles/5661032-audit-logs.
    - Voor KiwiHR SaaS:
        - Instructies voor het bekijken van een logboek met de wijzigingen in de gegevensinvoer in het profiel van de werknemer worden hier verder uitgelegd:
            - https://support.kiwihr.com/en/articles/9345331-kiwihr-plus-features#h_624211bc16
    - Voor Javelo SaaS:
        - Het is mogelijk om de voortgang van de campagne bij te houden. Instructies voor het bekijken van rapporten zijn hier te vinden:
            - 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
    - Houd er rekening mee dat niet alle logboeken beschikbaar zijn via de functie auditlogs. Gedetailleerde logboeken zijn op aanvraag beschikbaar
- De toegang van Tellent-medewerkers tot accounts van klanten wordt geregistreerd. Werknemers hebben over het algemeen alleen toegang tot accounts na toestemming van de eindgebruiker.
- De Tellent-applicaties worden automatisch gemonitord en (ver)storingen worden 24/7 opgevolgd door de ingenieurs van Tellent.
    - De status van de Tellent-applicaties kan worden gecontroleerd via https://status.tellent.com.
- Geautomatiseerde tests worden opgezet door het kwaliteitszorgteam om automatisch te controleren of de applicatie naar behoren werkt.
- De toegang tot servers onder het beheer of de controle van Tellent wordt geregistreerd.
- Inbraakdetectiesystemen zijn aanwezig.

Noodherstel, back-up en redundantie

- Er bestaat een Back-up en Herstelbeleid voor Tellent.
- Webservers worden redundant opgezet en automatisch geschaald.

- Bestandshosting is uiterst schaalbaar opgezet door gebruik te maken van Amazon S3.
- Versleutelde back-ups worden minimaal dagelijks gemaakt van alle door de klant beheerde gegevens en worden verwijderd wanneer ze niet langer redelijkerwijs nodig zijn.
- Back-ups worden opgeslagen in verschillende datacenters.
- Alle datacenters die door Tellent worden gebruikt , hebben een noodherstelplan.

Hostingproviders en datacenters

- Tellent gebruikt het Google Cloud Platform en Amazon Web Services om de Tellent-applicaties te hosten.
- De diensten die door Google Cloud Platform en Amazon Web Services aan Tellent worden geleverd, zijn ISO 27001- en CSA STAR-gecertificeerd en voldoen aan SOC 2 (SSAE 16/ISAE 3402 Type II).
- Andere sub-verwerkers of leveranciers van hostingdiensten zijn ook ISO 27001-gecertificeerd en/of voldoen aan de SOC 2 (SSAE 16/ISAE 3402 Type I)-standaard.
    - Meer informatie kunt u vinden in onze DPA.
- Er zijn sterke fysieke controles aanwezig voor alle datacenters.
- Alle gegevens in datacenters worden professioneel verwijderd na buitengebruikstelling van hardware.

Kantoren

- Kantoren zijn beveiligd met een combinatie van camera's, alarmen, beveiligingsmedewerkers en/of toegangspassen/kaartjes.
- Alle laptops van werknemers worden door het bedrijf beheerd (MDM) en zijn beschermd tegen toegang tot gegevens door onbevoegde personen.

Organisatie en beheer, beveiligingsbeleid en -processen

- Medewerkers van Tellent zijn verplicht om hun schermen te vergrendelen wanneer ze niet bij hun scherm zijn.
- Tellent streeft naar een papierloos kantoor.
- Alle Tellent-medewerkers moeten akkoord gaan met de vertrouwelijkheidsvoorwaarden (zoals een geheimhoudingsverklaring - NDA)
- Medewerkers van Tellent zijn verplicht om uitsluitend sterke wachtwoorden te gebruiken.
- Apparaten van Tellent-medewerkers hebben antivirussoftware en versleuteling.
- Er zijn toegangscontrolebeleidsmaatregelen getroffen om ervoor te zorgen dat de toegang wordt ingetrokken wanneer Tellent-medewerkers het bedrijf verlaten. Het principe van de minste privileges wordt toegepast en actief gemonitord.
- Beveiligingsbewustzijn wordt actief bevorderd binnen Tellent door middel van regelmatige trainingen.

Reactie op incidenten

- Er bestaat een Security Incident Response Plan (SIRP) voor Tellent.
- Het SIRP bevat een duidelijke aanduiding van autoriteit, stappen die moeten worden ondernomen in geval van een incident en een lijst met interne en externe leden van het Response Team.
- Het SIRP dekt ook de reacties op datalekken, zoals vereist onder de AVG.
- Incident (tafelexercise) oefeningen worden regelmatig uitgevoerd met relevante belanghebbenden.

Serviceniveau en ondersteuning

- Tellent streeft naar een beschikbaarheid van 99,5%, exclusief onderhoud. Het trackrecord van Tellent is hier te vinden: https://status.tellent.com
- Het ondersteuningsteam van Tellent is beschikbaar tussen 9.00 en 18.00 uur (CET en EST), per e-mail en livechat.
- Onze helpdeskartikelen op https://support.tellent.combieden richtlijnen voor elke update.
- Grote productwijzigingen worden gecommuniceerd via e-mails en/of de in-app ondersteuningschat door ons klantenserviceteam.
- Productroadmaps zijn te vinden op: https://support.tellent.com/en/articles/9805760-tellent-hr-platform-roadmap-2024

Definities

- Eindgebruikers: alle gebruikers behalve bezoekers van de Vacaturesite, kandidaten en verwijzers.

Disclaimer: dit document is bedoeld om de lezer een algemeen overzicht te geven van de beveiligings-, nalevings- en operationele maatregelen die door Tellent zijn genomen met betrekking tot de dienst(en) op de "Laatst bijgewerkt"-datum. Sommige onderscheidingen of nuances kunnen over het hoofd worden gezien. Neem contact op met Tellent voor meer specifieke en/of actuele informatie.