Tellent Whitepaper
Security, Compliance & Operations

With this document, Tellent provides you transparency and clarity on its security, compliance and operations policies that form the foundations of our business and partnerships. Because we know that engaging a service provider is an important business decision and that, like any partnership, it should be built on trust.

In this document, you can expect a general overview of the security measures taken by Tellent as an organization and in the Tellent Software as a Service products/modules:

- KiwiHR by Tellent, a core human resources system
- Javelo by Tellent, a performance management system
- Recruitee by Tellent, an applicant tracking system
- Any other service that provides unified functionality between the above-mentioned products/modules.

For questions, please contact the Tellent via the in-app support chat, or the Security Team directly via: security@tellent.com

tellent

Table of Contents

tellent

Compliance, Certifications, and Audit reports

ISO 27001 certification and SOC 2 assurance report

Tellent:

- ISO 27001:2022
  - A copy of Tellent's ISO 27001 certification can be found here.
  - Tellent's ISO 27001 statement of applicability can be found here.
  - Scope of Tellent's ISO 27001 certificate: *The secure development, operation and delivery of the following Tellent Software as a Service products/modules: Core human resources information system (also marketed under the brand name "KiwiHR"), performance management (also marketed under the brand name "Javelo"), applicant tracking system (also marketed under the brand name "Recruitee") and any product/module that provides unified functionality between those products/modules.*

Recruitee SaaS:

- SOC 2
  - A copy of Recruitee's SOC 2 (SSAE 16/ISAE 3402 Type II) report can be shared on request.

Internal auditing and penetration tests

- Tellent's Information Security Officer (ISO), together with various specialized third-party auditors, audit the security of the services and company processes.
- Penetration tests are performed regularly by esteemed security firms.
- Customers may perform their own penetration tests and audits on request.

GDPR

- Tellent facilitates your ability to comply with GDPR, including by offering dedicated GDPR features.
  - Our dedicated Customer Success managers and support team is able to assist with the configuration and to answer any feature related questions.
- Our standard Data Processing Addendum (DPA) forms part of the agreement between Tellent and you as a customer, unless explicitly agreed otherwise.
- Tellent's GDPR compliance is monitored by Tellent's internal legal department.
- All personal data processed on behalf of our customers is stored within the European Union and shall not be transferred to third countries without your approval.
- Tellent only complies with governmental requests for access to (personal) data insofar it is legally required to do so under applicable laws and regulations.

Customer data (including customer personal data)

- Customer data is any data, including personal data, processed by Tellent on behalf of a customer as part of the SaaS, excluding back-ups.

- In relation to customer personal data specifically, customers are considered the data controller of such personal data and Tellent the data processor, as further defined in our Data Processing Addendum (DPA).
- Tellent never sells, advertises, or uses customer data in any other way than to perform or improve the services provided to its customers.
- Customers may export customer data by using Tellent's APIs or any export features made available as part of the SaaS.

Application Security

Identity and Role based access

The status of, or access to, roles and permissions of members can be set within the Tellent Admin Center and/or individually via the Recruitee SaaS, Javelo SaaS or KiwiHR SaaS.

Through these various settings, it is (for example) possible to:

- In the Recruitee SaaS, limit open job position information to hiring managers only;
- In the Javelo SaaS, only display the status or results of open surveys or campaigns to employees that are part of your HR team;
- In the KiwiHR SaaS, allow only the data and details of an employee to be shown to their direct manager;
- From the Recruitee SaaS, share candidate data with non-users using unique links;
- In the Recruitee SaaS, apply visibility features to profile fields of candidates that applied to, for example, protect salary indications from being visible.

The support article containing more information on managing account settings on the **Tellent Admin Center** can be found on:
https://support.tellent.com/en/collections/9447061-account-settings

The support article containing more information on managing account settings in the **Javelo SaaS** can be found on: https://support.javelo.com/en/collections/9545584-account-settings

The support article containing more information on managing user roles in the **KiwiHR SaaS** can be found on: https://support.kiwihr.com/en/articles/9345339-user-roles & https://support.kiwihr.com/en/articles/9345338-access-levels

The support article containing more information on user roles (hiring roles) in the **Recruitee SaaS** can be found on: https://support.recruitee.com/en/articles/1066251-hiring-roles

Security of data in transit and encryption

- All data is transferred over the internet using TLS 1.2 or higher with a public key size of 2048 bits minimum.
- Cookies with sensitive information are set with "secure" and "http-only".
- Customer data is encrypted at rest (AES 256 or better).

tellent

Secure coding

- Developer efforts are aimed at mitigating OWASP top 10 risks and following industry best practices for security.
- Automated tests are set up to automatically check that the application functions as it should.
- Automation has been set up to automatically check for vulnerabilities in code and dependencies.
- New code is tested by Tellent's quality assurance team.
- Production data is never used for testing. Tellent has a separate staging environment(s).
- All code is subject to code review.

Malware and cross-site-scripting protection

- Uploads of files by candidates and End-Users are scanned for malware. Definitions are updated automatically and regularly.
- Data from user input fields is sanitized.
- Developers follow best practices, such as the OWASP Top 10, to prevent Cross Site Scripting (XSS), SQL injection (SQLi) and Cross Site Request Forgery (CSRF).

Authentication

- It is possible to integrate your own Single Sign On identity provider (via SAML 2.0)
    - For accounts without SSO, logins are based on the email address and password of the End-User.
    - New passwords must be at least 8 characters, including each of the following types of characters: uppercase letter, lowercase letter, and number.
- Once successfully authenticated, an access token is granted.
    - Each End-User device is provided a different, individual, access token.
    - Tokens are stored securely (cookies, "secure" and "http-only")
- All access tokens are revoked when a user changes their password. This includes password changes through the "forgot password"-functionality.
- Access tokens expire after 30 days and are revoked after an End-User logs out. Old access tokens are regularly replaced with new access tokens during continued use of the app.
- Tellent only stores hashes of passwords for user accounts, not the passwords themselves. Hashes are generated using a strong industry standard algorithm and generated according to best practices.
- After a high number of login attempts on one account it will be temporarily blocked.

E-mail protection

- The outgoing and incoming e-mail servers of Tellent support TLS.
- SPF, DMARC and DKIM are used for all outgoing mail.
- The customer can fully control the security of the email integration by connecting the Recruitee SaaS to their own IMAP- and SMTP-server over TLS. That would also allow the customer to benefit from SPF, DKIM and DMARC.

- The Recruitee SaaS also has functionality to share candidates to non-users via HTTPS instead of less secure e-mail protocols.

Hosting, technical and physical infrastructure

Protection of Servers and Infrastructure

- A minimal amount of public IP-addresses is used. Only front-end servers have public IP-addresses.
- Firewalls are in place. The implementation is covered by a policy.
- Google Cloud Platform and Amazon Web Services infrastructure mitigates and absorbs all Layer 4 and below (D)DOS attacks.
- Automated and manual processes have been set up to scan and detect vulnerabilities in server software packages and to regularly update such packages.

Multi-tenancy

- Tellent's SaaS offering is provided in a multi-tenant environment that is logically separated. This offers an economy of scale and means Tellent can invest a lot in measures to protect your account against peaks in traffic.
- The logical separations are tested by Tellent's quality assurance team and during a third party penetration test.
- At this point Tellent doesn't offer single tenant solutions.

Logging and Monitoring

- Many activities of End-Users can be tracked in the product.
- Every API call is logged. The Tellent applications are fully based on interactions with the API(s).
    - The Tellent applications offer an audit logs feature that allows administrators to view logs for a great amount of events in the application.
    - For the Recruitee SaaS:
        - A list of the events that are logged is available on the following page:
            - https://docs.recruitee.com/docs/audit-logs.
        - More general information about the audit logs feature can be found here:
            - https://support.recruitee.com/en/articles/5661032-audit-logs.
    - For the KiwiHR SaaS:
        - Instructions on how to view a log of the data entry changes to the employee's profile is further explained here:
            - https://support.kiwihr.com/en/articles/9345331-kiwihr-plus-features#h_624211bc16
    - For the Javelo SaaS:
        - It is possible to track campaign progress. Instructions on how to view reports can be found here:
            - 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
    - Please note that not all logs are available through the audit logs feature. Detailed logs are available on request
- Access of Tellent employees to customer owned accounts is logged. Employees are generally only permitted to access accounts after receiving the End-User's consent.
- The Tellent applications are automatically monitored and disruptions are followed up 24/7 by Tellent's engineers.
    - Status of the Tellent applications can be monitored via https://status.tellent.com.
- Automated tests are set up by the quality assurance team to automatically check that the application functions as it should.
- Access to servers under the management or control of Tellent is logged.
- Intrusion detection systems are in place.

Disaster Recovery, Backup, and Redundancy

- A Backup & Recovery Policy for Tellent is in place.
- Web servers are set up redundantly and scale automatically.
- File hosting is set up extremely scalable by using Amazon S3.
- Encrypted backups are made at least every day of all customer owned data and deleted when no longer reasonably necessary.
- Backups are stored in different data centers.
- All data centers used by Tellent have a disaster recovery plan.

Hosting providers & data centers

- Tellent uses Google Cloud Platform and Amazon Web Services to host the Tellent applications.
- The services provided by Google Cloud Platform and Amazon Web Services to Tellent are ISO 27001 and CSA STAR certified, and SOC 2 (SSAE 16/ISAE 3402 Type II) compliant.
- Other hosting sub-processors or suppliers are also ISO 27001 certified and/or SOC 2 (SSAE 16/ISAE 3402 Type I) compliant.
    - Further details can be found in our DPA.
- Strong physical controls are in place for all data centers.
- All data in data centers is professionally deleted after decommissioning of hardware.

Offices

- Offices are secured with a combination of cameras, alarms, security guards and/or keycards/keytags.
- All employee laptops are company managed (MDM) and have been protected against access to data by unauthorized individuals.

Organization and Management, Security Policies and Processes

- Tellent employees are required to lock their screens when they are away from their screens.
- Tellent strives to have a paperless office.
- All Tellent employees are required to agree to confidentiality conditions (such as an NDA).
- Tellent employees are required to exclusively use strong passwords.
- Tellent employee devices have anti-virus software and encryption.
- Access control policies are in place to make sure that access is revoked when Tellent employees are offboarded. The least privilege principle is applied and actively monitored.
- Security awareness is actively cultivated within Tellent with regular training.

Incident Response

- A Security Incident Response Plan (SIRP) for Tellent is in place.
- The SIRP contains a clear designation of authority, steps to be taken in case of an incident and a list of internal and external members of the Response Team.
- The SIRP also covers responses to data breaches such as required under the GDPR.
- Incident (table-top) exercises are performed with relevant stakeholders on a regular basis.

Service level and support

- Tellent aims for a 99.5% uptime excluding maintenance. Tellent's track record can be found here: https://status.tellent.com
- Tellent's support team is available between 9am and 6pm (CET and EST), per e-mail and live chat.
- Our help desk articles on https://support.tellent.com provide guidance on every update.
- Big product changes are communicated via emails and/or the in-app chat service by our customer support team.
- Product roadmaps can be found on: https://support.tellent.com/en/articles/9805760-tellent-hr-platform-roadmap-2024

Definitions

- End-Users: All users except visitors of the Careers Site, candidates and referrers.

Disclaimer: This document is intended to give the reader a general overview of security, compliance and operational measures taken by Tellent in relation to the service(s) on the "Last updated"-date. Some distinctions or nuances may be overlooked. Please contact Tellent for more specific and/or up to date information.