talentcloud.ai

TALENTCLOUD.AI SECURITY AND DATA PRIVACY

Talent Acquisition	Employee Onboarding & Management	Employee Retention & Development	Business Data Analytics

As business becomes increasingly digital, securing and protecting customer, employee, and intellectual property data is a top priority for IT leaders. And with organizations facing more sophisticated security threats, it's critical to deliver security and data privacy across all aspects of service. Here is an introduction to Talentcloud.ai practices across security and data privacy for IT professionals.

PHYSICAL SECURITY

Talentcloud.ai co-locates its production systems in state-of-the-art data centers designed to host mission-critical computer systems with fully redundant subsystems and compartmentalized security zones. Talentcloud.ai data centers adhere to the strictest physical security measures:

- Multiple layers of authentication are required before access is granted to the server area.
- Critical areas require two-factor biometric authentication.
- Camera surveillance systems are located at critical internal and external entry points.
- Security personnel monitor the data centers 24/7.
- Unauthorized access attempts are logged and monitored by data center security.

All physical access to the data centers is highly restricted and stringently regulated. Talentcloud.ai data operations use security best practices such as "least access" hardened servers and regularly scheduled maintenance windows.

DATA SEGREGATION

Talentcloud.ai is a multi-tenant SaaS application.

Multi-tenancy is a key feature of Talentcloud.ai that enables multiple customers to share one physical instance of the Talentcloud.ai system while isolating each customer tenant's application data. Talentcloud.ai accomplishes this through the Talentcloud.ai Object Management Server (OMS). Every user ID is associated with exactly one tenant, which is then used to access the Talentcloud.ai application.

All instances of application objects (such as Organization and Worker) are tenant-based, so every time a new object is created, that object is also irrevocably linked to the user's tenant. The Talentcloud.ai system maintains these links automatically and restricts access to every object, based on the user ID and tenant. When a user requests data, the system automatically applies a tenancy filter to ensure that it retrieves only information corresponding to the user's tenant.

ENCRYPTION OF DATA AT REST (DATABASE SECURITY)

Talentcloud.ai encrypts every attribute of customer data within the application before it is stored in the database. This is a fundamental design characteristic of the Talentcloud.ai technology. Talentcloud.ai relies on the Advanced Encryption Standard (AES) algorithm with a key size of 256 bits. Talentcloud.ai can achieve this encryption because it is an in-memory object-oriented application as opposed to a disk-based RDBMS application. Specifically, metadata in Talentcloud.ai is interpreted by the Talentcloud.ai OMS and stored in memory. All data inserts, updates, and deletes are committed to a persistent store on a MySQL database. This unique architecture means Talentcloud.ai operates with only a few dozen database tables. By contrast, a RDBMS- based application requires tens of thousands of tables, making complete database encryption impractical due to its detrimental impact on performance.

ENCRYPTION OF DATA IN TRANSIT (NETWORK SECURITY)

Users access Talentcloud.ai via the internet, protected by Transport Layer Security (TLS). This secures network traffic from passive eavesdropping, active tampering, and forgery of messages.

Talentcloud.ai has also implemented proactive security procedures, such as perimeter defense and network intrusion prevention systems. Vulnerability assessments and penetration testing of the Talentcloud.ai network infrastructure are also evaluated and conducted on a regular basis by both internal Talentcloud.ai resources and external third-party vendors.

DATA BACKUPS

The Talentcloud.ai primary production database is replicated in real time to a secondary database maintained at an off-site data center. A full backup is taken from this secondary database each day. Our database backup policy requires database backups and transaction logs to be collected so that a database can be recovered with the loss of as few committed transactions as is commercially practicable. Transaction logs are retained until there are two backups of the data after the last entry in the transaction log. Database backups of systems that implement interfaces must be available as long as necessary to support the interfacing systems. This period will vary by system. Backups of the database and transaction logs are encrypted for any database that contains customer data.

DISASTER RECOVERY

Talentcloud.ai warrants its service to its standard service-level agreement (SLA). The SLA includes a disaster recovery (DR) plan for the Talentcloud.ai Production Service with a recovery time objective (RTO) of 12 hours and a recovery point objective (RPO) of 1 hour. The RTO is measured from the time the Talentcloud.ai Production Service becomes unavailable until it is available again. The RPO is measured from the time the first transaction is lost until the Talentcloud.ai Production Service became unavailable.

To make sure Talentcloud.ai maintains these SLA commitments, Talentcloud.ai maintains a DR environment with a complete replication of the production environment. In the event of an unscheduled outage where the outage is estimated to be greater than a predefined duration, Talentcloud.ai executes its DR plan. The DR plan is tested at least every six months.

SINGLE-SIGN-ON SUPPORT

While LDAP allows for a unified username/password solution, SAML takes the next step by enabling an enterprise SSO environment. SAML allows for a seamless SSO experience between the customer's internal identity and access management (IAM) solution and Talentcloud.ai.

ONE SECURITY MODEL

Unlike legacy ERP systems, Talentcloud.ai operates on a single security model. This includes user access, system integration, reporting, mobile devices, and IT access. Everyone must log in and be authorized through the Talentcloud.ai security model. By contrast, in legacy ERP systems, there typically is an applications layer of security that IT and DBA personnel can bypass to access the data directly at the database level. This is not possible with Talentcloud.ai. Talentcloud.ai is an object-oriented in-memory system with an encrypted persistent data store. As a result, access events and changes are tracked and audited. This uniquely robust security model, combined with the automatic ability to effectively date and audit all data updates, shortens the time and lowers the costs associated with governance and compliance and reduces overall security risk.

AUTHENTICATION

Talentcloud.ai security access is role-based, supporting SAML for single-sign-on (SSO) and x509 certificate authentication for both user and web services integrations. Talentcloud.ai allows customers to set up different authentication requirements for different user populations.

Talentcloud.ai also enables users to select an authentication type in situations where organizations wish to use multiple authentication types for users, due to geographical and/or organizational variances.

TALENTCLOUD.AI NATIVE LOGIN

For customers who wish to use the native login, Talentcloud.ai stores their Talentcloud.ai password only in the form of a secure hash, rather than the password itself. Unsuccessful login attempts as well as successful login/logout activity are logged for audit purposes. Inactive user sessions are automatically timed out after a specified time, which is customer-configurable by user. Customer-configurable password rules include length, complexity, and expiration.

MULTIFACTOR AUTHENTICATION

Talentcloud.ai provides and recommends that customers use multifactor authentication (MFA). Talentcloud.ai allows customers to supply any authenticator application backed by the Time-Based One-Time Passcode (TOTP) algorithm. With this setup, customers can easily integrate MFA providers with the Talentcloud.ai native login. Talentcloud.ai also allows end users of customers to receive a one-time passcode delivered via an email-to-SMS gateway mechanism.

Lastly, Talentcloud.ai supports challenge questions as an additional mechanism to prove a user's identity.

TRUSTED DEVICES

Talentcloud.ai provides the ability for customers and their end users to enroll devices as trusted for access to their Talentcloud.ai tenant. End users will be notified of unrecognized devices attempting to access their account. They will have the ability to remove devices they no longer trust. For administrators, a list of trusted devices is provided for monitoring purposes. End users must consent to tracking of the trusted device with a browser cookie.

STEP-UP AUTHENTICATION

Talentcloud.ai provides step-up authentication as a stronger authentication mechanism for access to sensitive resources. Organizations using SAML as an authentication type can further ensure that data is secured against unauthorized access to items within Talentcloud.ai deemed critical. This allows customers to force a secondary authentication factor that users must enter to access those items.

AUTHORIZATION

The Talentcloud.ai application enforces group policy-based security for authorization. The application prevents any user from directly accessing the production database. Talentcloud.ai-delivered and customer-created security groups, combined with predefined security policies, grant or restrict user access to functionality, business processes, reports, and data—whether accessed online or through web services.

Customer-configurable security groups are based on users, roles, jobs, organizations, location hierarchy, or business sites. They can be combined into new security groups that logically include and exclude other groups. System-to- system access is defined by integration system security groups. Customers can tailor these groups and policies to meet their needs, providing as fine-grained access as required to support complex configurations, including global implementations.

Talentcloud.ai also provides security groups that are automatically updated on the basis of business processes, such as hire and end contract. These Talentcloud.ai-delivered groups can be used alone or in combination with other Talentcloud.ai- delivered or customer-created security groups to determine access via security policies.

PUBLIC CLOUD

Talentcloud.ai uses public cloud services from Amazon Web Services (AWS) for storing and processing content in Talentcloud.ai Media Cloud. Customer content is logically segregated from that of other customers. All Talentcloud.ai Media Cloud content is encrypted at rest, using AWS's server-side encryption. Each object Talentcloud.ai stores within AWS is encrypted with AES with a unique 256-bit encryption key.

Talentcloud.ai uses Amazon Virtual Private Cloud (Amazon VPC), which is a logically isolated section of the AWS cloud. All communication between end users to Talentcloud.ai data centers and Talentcloud.ai Amazon VPC services is encrypted at the transport layer. Additionally, all of the communication from Talentcloud.ai Amazon VPC services to Talentcloud.ai data centers and vice versa is encrypted as well. Talentcloud.ai uses the TLS protocol to encrypt all the traffic with secure ciphers only.

ALWAYS-ON AUDITING

Talentcloud.ai tracks all changes to business data at the application level. This application audit information is the basis for audit and compliance reporting found throughout the Talentcloud.ai system. Talentcloud.ai records successful logins and logouts by users as well as unsuccessful login attempts and provides this information in Talentcloud.ai audit reports. Talentcloud.ai uses nondestructive updates, which means data is never overwritten and is maintained for the lifetime of the tenant. This enables customers to obtain a complete audit history of any value. The auditing features in Talentcloud.ai provide an auditor with the information required to trace the history of changes made to a business object or transaction.