TALENTERIA

Talenteria

Security Datasheet

Table of Contents

1 Overview

Talenteria is an innovative AI-driven recruitment platform designed to transform the way businesses attract, engage, and hire top talent. In the digital era, where data is a critical asset, ensuring the security and privacy of this data is paramount. This overview provides a snapshot of the security measures and policies Talenteria employs to safeguard information and maintain the highest data integrity and confidentiality standards.

2 Infrastructure security

2.1 Azure Cloud Platform

Talenteria software and databases are hosted in Microsoft Azure, the most trusted data center on the market. With over 90 Security Compliance Certifications, Azure allows Talenteria to provide an efficient and comprehensive recruiting platform no matter where you are located, and no matter what industry you are in.

Learn more about Microsoft Azure Security:

https://azure.microsoft.com/en-ca/explore/security

2.2 Software Updates and Upgrades

We adopt a proactive stance in updating our software, anticipating and addressing potential security threats before they impact our users. Our team continuously monitors for vulnerabilities, bugs, and performance issues, ensuring timely and effective responses.

Update Frequency and Scheduling

- Regular Updates: Talenteria undergoes regular software updates to enhance functionality, address bugs, and patch vulnerabilities.
- Scheduled Maintenance: Major upgrades are scheduled during off-peak hours to minimize disruption to our users. Users are notified in advance of any significant updates.

Types of Updates

- Security Updates: These are prioritized and implemented swiftly to mitigate any vulnerabilities and enhance the platform's defense against cyber threats.
- Feature Updates: Regular updates that introduce new functionalities, improve existing features, and ensure the platform remains user-friendly and efficient.
- Performance Updates: Focus on optimizing the platform's speed, scalability, and reliability.

2.3 Antivirus Policy

This policy is designed to protect the organizational resources against intrusion by viruses and other malware.

Systems must have the Talenteria standard virus runtime scanning software loaded and running at all times. At no time may a system on a hosting network have the virus scanning software and update virus definitions disabled.

Support Engineers use the Antivirus Remote Management Console for central administration of Antivirus defense on all systems.

3 Data security

3.1 Data Transfer

All connections between users, applications, and backend services are secured by HTTPS/SSL certificates. We use industry-standard Transport Layer Security (TLS) 1.2 or later protocol with 2,048-bit RSA/SHA256 encryption keys, as recommended by CESG/NCSC, to encrypt communications between the internal systems and datacenters, as well as communication from the customer to the cloud.

3.2 Data Isolation

Our system is designed to manage and allocate cloud resources for our clients effectively and securely. We employ a robust framework that ensures each client's data is logically isolated from that of others into separate databases. This segregation guarantees the confidentiality of each client's data, preventing access by other clients.

When utilizing our services, your data is stored on our servers. It is important to note that the ownership of this data remains solely with you, the user, and not with Talenteria.

3.3 Data Backup

The purpose of this policy is as follows:

- To safeguard the Client’s information assets;
- To prevent the loss of data in the case of an accidental deletion or corruption of data, system failure, or disaster;
- To permit timely restoration of information and business processes, should such events occur.
- To manage and secure backup and restoration processes and the media employed in the process.

This policy applies to all Client’s data in the Talenteria Azure Network.

Talenteria uses two steps of backup:

- SQL server backup – every night makes a local backup of Client’s database;
- Azure Recovery Services Vaults – every night makes a backup to Azure Geo-redundant storage (GRS).

4 Identity and access control

4.1 Firebase Authentication Provider

Talenteria authentication is powered and integrated with Firebase (https://firebase.google.com/). Firebase Authentication is certified under major privacy and security standards:

- ISO 27001
- ISO 27017
- ISO 27018
- SOC 1
- SOC 2

- SOC 3

Learn more about Firebase Security:

https://firebase.google.com/support/privacy

4.2 Role-Based Access Control (RBAC)

Role-based access control (RBAC) enables you to grant access based on the user's assigned role, making it easy to give users only the amount of access they need to perform their job duties.

Database and server access is limited and allowed only to Talenteria engineers.

5 AI Security

Talenteria is integrated and empowered by OpenAI to provide advanced and secure AI-driven technologies.

All data processed through OpenAI's systems are managed under strict privacy controls and security protocols to prevent unauthorized access and data breaches.

Learn more about OpenAI security: https://openai.com/security

6 Operational security

6.1 Logging and Monitoring

Talenteria uses application-level logging and Azure / OS-level logging.

- Application-level logging: All user actions inside the Talenteria application are recorded into an audit log/trail.
- Azure / OS-level logging: System events

All security-related events on critical or sensitive services and applications must be logged and audit trails saved.

Talenteria engineers monitor:

- CPU utilization, Active processes;
- File store - utilization, anomalies, file types and file sizes;
- Network statistics e.g., peak and average bandwidth utilization and errors;
- System and security log anomalies;
- Unsuccessful access attempts;
- Successful access attempts - user account, date/time stamp, session duration;
- Unusual network traffic.

Support engineers will receive an email alert when:

- One or more critical services are unavailable or have errors;
- Backup procedure did not execute properly;
- Virus or other malware found;

6.2 SDLC

Standardizing the development approach and coding techniques for critical systems will ensure their maintainability, security, protection against cyber-attacks and accessibility.

Information security is integrated throughout the Talenteria Software Development Life Cycle (SDLC) methodology used when developing the Talenteria core system, any custom client solutions, web-based administration interfaces, internal and external applications, or any other application where restricted or confidential information assets may be stored, processed, or transmitted.

SDLC methodology, processes and procedures cover the following aspects:

- Development process and methodology
- Code Reviews
- Separation of Environments
- Quality Assurance processes
- Migration to the Production environment

6.3 Handling Incidents

At Talenteria, we recognize the critical importance of effective incident management to maintain the security and integrity of our platform.

Incident Response Procedure

- Initial Assessment: Upon detection of a potential incident, an immediate assessment is conducted to determine its nature and scope.
- Containment: Swift actions are taken to contain the incident and prevent further spread or damage.
- Eradication: Identifying and eliminating the root cause of the incident to prevent recurrence.
- Recovery: Restoring affected services to full functionality while ensuring no lingering threats remain.

6.4 Penetration Tests

Talenteria places a high priority on the security of its platform, and a key component of this commitment is security testing. We employ a comprehensive suite of testing methodologies, including penetration testing, vulnerability scanning, and code reviews, to proactively identify and address potential security weaknesses.

Our team regularly conducts these tests, simulating real-world attack scenarios to ensure our defenses remain robust against evolving cyber threats. Additionally, we engage third-party security software for independent assessments, ensuring an unbiased evaluation of our security posture.

7 Organizational security

7.1 HR Security Policies

Talenteria’s commitment to security extends into the realm of human resources, where we have established a series of HR Security Policies designed to safeguard sensitive information and maintain the integrity of our recruitment platform. These policies include:

- Access Control Policy: Implementing strict access controls to ensure employees have access only to the information necessary for their role, thereby minimizing the risk of internal data breaches.
- Confidentiality Agreements: Mandatory signing of confidentiality agreements by all employees to legally bind them to the responsible handling of sensitive information.
- Regular Audits of HR Practices: Frequent audits of HR practices and procedures to identify and rectify any potential security gaps.
- Incident Reporting Mechanism: A clear and accessible mechanism for employees to report any security concerns or breaches, ensuring prompt action can be taken.
- Offboarding Procedures: Secure and thorough offboarding processes for departing employees to ensure the return of company assets and the revocation of access to Talenteria systems.

These policies form a critical part of Talenteria's overarching security strategy, ensuring that our human resources operations align with our high standards of data protection and cybersecurity.

7.2 Employment Security

HR team ensures that potential users are recruited in line with the recruitment and selection policy for the roles they are considered for and to reduce the risk of theft, fraud, or misuse of information or information systems by those users.

The HR team conducts background verification checks on all candidates for employment, including contractors and third-party users, and these checks shall be carried out in accordance with relevant laws.

7.3 Security Training

Regular training sessions for all employees, focusing on cybersecurity best practices, data protection regulations, and the importance of maintaining strict security protocols.