Security Statement

Version 1.7

Last Updated: 26th April 2018

great{with}talent

www.greatwithtalent.com ▫ info@ greatwithtalent.com ▫ +44 (0) 333 012 4649

Introduction

This Security Statement applies to the products, services, websites and apps offered by GreatWithTalent Ltd ("great{with}talent"). We refer to those products, services, websites and apps collectively as the "Services" in this Statement. This Security Statement also forms part of our Terms of Service for our clients.

We value the trust that our customers place in us by letting us act as processors of their data. We take our responsibility to protect and secure your information very seriously. Our Privacy Policy also further details the ways we handle your data.

Physical Security

Data collected through great{with}talent is located on servers in state-of-the-art data centres with the latest in redundant power, environmental controls and networking technologies.

Trained professionals safeguard the security of the equipment by staffing this facility around the clock. Physical security controls at our data centres include 24x7 monitoring, cameras, visitor logs, and entry requirements.

Security Policies

great{with}talent maintains and regularly reviews and updates its information security policies on an annual basis. Employees must acknowledge policies on an annual basis and undergo additional training and job specific security and skills development and/or privacy law training for key job functions. The training schedule is designed to adhere to all specifications and regulations applicable to great{with}talent.

great{with}talent is also working towards ISO 27001 certification.

Data Access & Control

Access to data, customer information and systems administration is limited by complex username and passwords or administrative privileges. All great{with}talent employees who may interact with customer data have been vetted by our rigorous onboarding screening processes. In addition, great{with}talent communicates its information security policies to all personnel, requires new employees to sign non-disclosure agreements, and provides ongoing privacy and security training. We revoke access upon employee termination.

Vulnerability Management & Penetration Tests

We maintain a documented vulnerability management program which includes daily and periodic scans, identification, and remediation of security vulnerabilities on servers, workstations, network equipment, and applications. All networks, including test and production environments, are regularly scanned using trusted third party vendors. Critical patches are applied to servers on a priority basis and as appropriate for all other patches.

We also conduct regular internal and external penetration tests and remediate according to severity for any results found.

Data Encryption

Our entire platform uses 256-bit SSL encryption and data is also encrypted at rest.

Candidates and users of our services are only identified by encrypted identity strings and limited personal information. Decryption routines are used only at point where data extraction and subsequent analysis takes place.

Development

Our development team employs secure coding techniques and best practices, focused around the OWASP Top Ten. Developers are formally trained in secure web application development practices upon hire and annually.

Development, testing, and production environments are separated. All changes are peer reviewed and logged for performance, audit, and forensic purposes prior to deployment into the production environment.

Logging and Auditing

Application and infrastructure systems log information to a centrally managed log repository for troubleshooting, security reviews, and analysis by authorised great{with}talent personnel. Logs are preserved in accordance with regulatory requirements. We will provide customers with reasonable assistance and access to logs in the event of a security incident impacting their account.

Asset Management

great{with}talent maintains an asset management policy which includes identification, classification, retention, and disposal of information and assets. Company-issued devices are equipped with full hard disk encryption and up-to-date antivirus software. Only company-issued devices are permitted to access corporate and production networks.

Information Security Incident Management

great{with}talent maintains security incident response policies and procedures covering the initial response, investigation, customer notification (no less than as required by applicable law), public communication, and remediation. These policies are reviewed regularly and tested bi-annually.

Breach Notification

Despite best efforts, no method of transmission over the Internet and no method of electronic storage is perfectly secure. We cannot guarantee absolute security. However, if great{with}talent learns of a security breach, we will notify affected users so that they can take appropriate protective steps. We are committed to keeping our customers fully informed of any matters relevant to the security of their account and to providing customers all information necessary for them to meet their own regulatory reporting obligations.

Business Continuity

great{with}talent methodically backs up all databases and file servers on a daily basis. We operate a backup schedule maintaining full and differential backups of all service databases. Backups are saved off-site and stored securely in multiple locations (our current backup service supplier is Microsoft Azure Backup). great{with}talent also employs redundant servers for immediate failover in the event of a server failure.

great{with}talent mirrors the production environment to allow rapid restoration from off-site backups in the event of a hardware or software failure. All of our contingency plans are tested at strict regular intervals and recent tests provided no areas for concern.

Your Responsibilities

Keeping your data secure also requires that you maintain the security of your account by using sufficiently complicated passwords and storing them safely. You should also ensure that you have sufficient security on your own systems.