Control Risks

VANTAGE Security Protocol

Control Risks ("we") provides online solutions for our clients ("you"). Our online solutions encompass Vantage Gateway. VANTAGE is a suite of third-party risk and compliance products specifically designed for organisations that interact and work with partners across different sectors and jurisdictions. From initial screenings to deeper levels of research and on-the-ground due diligence, VANTAGE enables you to focus your efforts on mitigating risk, while building efficiencies and automation in your third-party risk management programme.

VANTAGE Gateway is an innovative, third-party risk-management application that combines unparalleled expertise, advanced technology, and the most reliable data, to help compliance professionals efficiently screen third parties, order due diligence reports, create portfolio risk dashboards, and manage compliance tasks for each entity in their portfolio.

This document explains what information we hold and how we secure the information.

The information we hold about your users

Personal data is collected direct from a data subject when they create their own profile and account for the purpose of accessing online solutions content through the website or mobile application.

Data provided by the data subject will include:

- First Name (mandatory)
- Last Name (mandatory)
- Business Email Address (mandatory)
- Phone Number (optional)
- Job Title (optional)

Further information regarding the types of personal information collected can be found in our **GDPR Narrative** document in the Trust Centre which also contains a data flow diagram for the VANTAGE services: https://www.controlrisks.com/legal-1/trust-centre

Login process

Users are required to log in to VANTAGE Gateway with a user-specific VANTAGE username and password.

Accounts that are hosted within the VANTAGE Gateway service enforce strong passwords (better than 14-character with complexity).

Clients have the option to enable multi-factor authentication (MFA). When enabled, all users associated with the client account are required to use MFA.

How we secure your information

Our strong set of security measures covers the people, process and technology required to assure the confidentiality, integrity, and availability of information. This includes policies; screening and training of our people; defined and audited processes; and extensive technological controls such as encryption, segmented data stores, data backups, firewalls, network and communication security, two-factor authentication for privileged access, and continuous monitoring.

VANTAGE Gateway undergoes 3rd party penetration testing annually, and sanitised reports can be made available upon request, subject to NDA signature.

We have an Information Security Management System (ISMS) run from head office, audited, and certified to ISO 27001 by BSI. This ISMS includes analysis of risks and legislative requirements, and assessment and implementation of appropriate mitigations on an ongoing basis.

Further information can be found in our Trust Centre https://www.controlrisks.com/legal-1/trust-centre

Hosting

- Our online solutions are hosted in Microsoft Azure Europe, which is certified to ISO 27001 and ISO 27018. These establish adherence to strict security controls and procedures. Microsoft Azure staff are security-screened as standard. Further information on Microsoft Azure security is available at: https://www.microsoft.com/en-us/trustcenter/compliance/iso-iec-27018.
- We manage our online solutions in Azure through a private cloud. The VANTAGE infrastructure is segregated from other Control Risks services – internal and external. From this perspective the service is self-contained.
- Physical access to the data centre locations by tenants is not permitted. Only Microsoft data centre technicians can access the data halls where the infrastructure is located. Access to physical datacentre facilities is protected by outer and inner perimeters with increasing security at each level, including perimeter fencing, security officers, locked server racks, multifactor access control, integrated alarm systems, and around-the-clock video surveillance by the operations centre. Premises are also protected by fire alarms and fire suppression systems.

Control Risks

VANTAGE Security Protocol

Infrastructure and security

- Online solutions have various technologies to protect the services, such as web application firewalls, DDOS protection, malware protection and monitoring agents.
- Online solutions are only hosted over HTTPS providing end-to-end encryption in transit between the client browser or mobile application and the Online application service.
- All client data within the online solutions are encrypted at rest.
- Online solutions are penetration/vulnerability tested at regular intervals by third-party testing companies that are CREST accredited.
- Security patches are applied on a regular defined schedule each month ensuring that the latest vendor security patches are implemented.
- Out of band ("OOB") security patches that are released outside of vendors' normal release schedule are assessed and applied as required.
- Software changes are peer-reviewed. Software and configuration changes go through a formal CAB (change advisory board) process before being deployed.
- Remote management access to the online solutions infrastructure is restricted to a defined list of employees, each with individual access accounts audited on a regular basis. No use of generic access accounts is permitted. Account passwords are reset on a regular scheduled basis.

Access controls – your end users

As explained in the Login Process section above.

- Each user is assigned a username (which must be an email address). New users receive a registration email which contains a unique link through which they can set a password.
- The link is valid for 14 days. A new link can be sent upon request.
- If the client has multi-factor authentication (MFA) enabled, new users associated with the client account will receive a welcome email with a link which will prompt verify their email address using a verification code.
- Upon verifying their email address, new users will be prompted to download an authenticator application to their smart mobile device and will register with the MFA solution and set a password.
- Current password restrictions are minimum of 14 characters. Passwords are encrypted and inaccessible.
- Users have access to a password reset function via the login page. If a recognised email address is provided, a secure password reset link is sent to that email address.

Access controls – our users

Gateway End Users

- Only VANTAGE Control Risks' staff in client facing roles have access to VANTAGE Gateway in order to demonstrate the functionality to clients / prospects.
- Internal users are setup in the same way as external users. That is, they receive a registration link and then set their own password.
- Internal accounts are only able to access non-Production/non-live (staging) environments.

MSA Administrators

- The administration of Gateway accounts/users takes place within the Managed Screening Application (MSA). Admin users inherit the same functionality as standard users, plus access to the administration site from where Gateway accounts and users can be setup/configured.
- Admin rights are restricted to users whose roles require them to be able to setup/modify accounts.
- Access to the MSA is via SSO with our corporate directory service, our directory service enforces strong passwords (better than 14-character with complexity), and locks out after repeated failed attempts to log in.

Client defined data: Third Parties

- The application includes functionality to add or upload third party information, individually or in bulk.
- Upload files are in Microsoft Excel format (.CSV).
- The client defined data is located on servers that are segregated and not publicly accessible. The only access to the data is via an application service that queries the asset data based upon the security of the client logon.
- Client defined data is stored in client-specific data stores referenced by individual client ID providing clear separation between the data of different clients.
- At no point is the individual client ID exposed within browser URLs.

If you have any further questions with regards to the security of our online services, please do not hesitate to contact your Control Risks' account manager or reach out to us at vantagesupport@controlrisks.com.