CARE ADVANTAGE DATA SECURITY, COMPATIBILITY, CUSTOMISATION AND PRIVACY

Care Advantage is a psychometric/behavioural screening assessment platform delivered as a web-application and compatible with most operating systems, browsers and devices. The platform can be skinned with the client's logo and colours and the client can customise some candidate messaging.

Data that is collected

The are 4 pieces of data collected as part of Care Advantage assessments

- First and last name for applicants
- Email Address (acts as a unique identifier)
- Raw assessment responses (Strings of alpha numeric code – anonymous and encrypted)

No business critical or sensitive data is collected. All data is encrypted, and our data exchanges are via Secure Socket Layers. We also utilize OAuth. Data is kept on secure servers and our processes comply with the GDRP requirements. The only Company information held is publicly available – Name and address. No data is sold or exchanged.

The digital journey

1. Candidate completes responses to assessments. Candidate agrees to terms of usage a part the assessments
2. Responses are encoded then encrypted on the Organisation's individual Dashboard
3. Dashboard sends code string to Assessment engine (always kept on separate server for security)
4. Assessment engine calculates scores and returns encoded digital string to User dashboard
5. Dashboard decodes the string and compiles the reports – matching them up to the ID number attached to the candidate

Compatibility	Response
On which devices can the assessments be completed?	Desktop Laptop Mobile phones Tablets
Which browsers (types and versions) are supported by the platform?	All
Which computer operating systems are supported by the platform?	All
Which (mobile) device operating systems are support by the platform?	All candidate screens and assessment screens support mobile responsive design.

Organisational	Response
Do you have an Information Security Management System Framework or equivalent in place?	Yes
Do you have an Information Security policy?	Yes
Does your organisation have an appointed Information Security Officer?	Yes, Paul Newman, paul@big5assessments.com
Do all users agree to an Information Systems Acceptable Use Policy prior to being granted access to systems?	Yes
Vulnerability Management	**Response**
Does your organisation conduct an annual penetration test of external systems and applications using an independent assessor?	Yes
Does your organisation ensure that vulnerabilities identified in the penetration tests are resolved?	Yes, all security issues raised are dealt with asap.
Do you ensure that all security related patches are applied immediately after release by the supplier/vendor (Operating Systems, Applications, Middleware and Toolset)	Yes
Data Storage, Business Continuity and Disaster Recovery	**Response**
Summarize the company's customer data hosting locations	AWS Hosting based in Dublin, Ireland.
Does the system have a logical or physical limit to the age or amount of information it stores?	Regarding capacity - no as the AWS EC2 volumes can be extended if required. In regard to age, this is in line with everything physically technological and is impossible to answer.
What is the lifecycle for data that transitions outside this limit?	As above
List the mechanisms by which data may be exported from the system in bulk.	There is the ability to generate different CSV data files.
Does the system offer direct access to the system's underlying data store? (example: able to make direct RDBMS connections and execute SQL query)	Only via secure connection and secure layer MVC model framework.
Please provide details about how often information will be backed up?	Full data backups daily
Please provide details on the how often backup recovery tests will be conducted and also critical systems supporting the service?	Annually
Is the system able to enforce so-called "policies" by locking configuration in a specific state?	All policies relating to system architecture are administered via AWS
List the configuration items that are not able to be enforced as policies.	All policies relating to system architecture are administered via AWS
Does your organisation have a disaster recovery process?	Yes
Does your organisation have a cyber insurance policy?	Yes

Application Development	Response
Do you use secure application development practices (secure coding)?	Yes
Do you have secure code reviews conducted or use peer reviews as part of your application development?	Yes
Threat Detection and Prevention	**Response**
Do you have an Intrusion Detection and/or Prevention System in operation which inspects all network traffic to/from systems that will store and process information?	Yes
Do you have a Firewall in operation to inspect all network traffic to/from systems that will store and process information?	Yes
Do you have a Firewall in operation to ensure that only authorised network traffic (including: connections, protocols and services) is permitted to/from systems that will store and process information?	Yes
Do you have Anti Malware (Anti-Virus) software installed on all client devices (including mobile devices, desktops & laptops) used to support & manage systems that will store and process information?	Yes
Do you have Anti Malware (Anti-Virus) software installed on all servers that will store and process information?	Yes
Do you have a Web Application Firewall (Layer 7) to protect Internet facing applications that are part of your systems that will store and process information?	Yes
Do you have any technologies in place to detect and prevent Advanced Persistent Threats (APTs) to information?	Yes
Do you ensure that all services not required on IT systems are disabled?	Yes
User Access Control	**Response**
What is the isolation level from one client's data from another?	Each client has their own separate platform with their own login.
Can the platform be set up with different access levels and authorisation levels (eg. Different offices/sites or users)	Yes, the system can be set up with different divisions and user can get access to all or 1 division. Each user can be set up with a certain authorisation level, limiting the functions in the platform.
Does the system support Role Based Access Control (RBAC)?	Yes – Admin, Managers, Guest, Candidate
Do you undertake a regular user access review?	Annually
Do you limit user access based on the least privilege principle?	Yes
Do you ensure that inactive user accounts are disabled after a specific period? (If so, how long)?	Yes, on termination, or 24 months, whichever is sooner.
Do you have an approval process for privileged account creation and modification?	Yes

Encryption	Response
Is information to be encrypted whilst in transit (transmission)?	Yes
Is information to be encrypted whilst at rest (storage)?	Partial, all Personal Identifiable Information and Passwords are encrypted.
Logging and Reporting	**Response**
Do you log security events to a centralised log server?	Yes
Do you generate alerts when security events occur that indicate actual or potential compromise/unauthorised activity on IT systems?	Yes
Within what timeframe are events and alerts investigated when they occur?	<4 hours
If a suspected or actual data breach was to occur, do you have a process for informing clients?	Yes
Within what period of time do you inform your clients of an actual or suspected data breach?	We have an investigation window (72hr) where we must notify relevant authorities and users.
API and Integrations	**Response**
Does the system expose an Application Programming Interface (API) for external access to the system?	Yes
Describe the available forms of this API (example: REST, SOAP over HTTP, COM)	REST OVER HTTPS
Does the API allow external systems to modify or act upon the system in the same way as the user interface?	In part - yes
List all the actions or modifications that are not available through this API.	Any - Session Authentication Methods Signature Authentication Methods Check Authorization Methods
Does the API provide an event-based integration mechanism such that the system will act upon or make contact with an external system as actions or modifications are made within the system?	Yes
Does it integrate with the Office365 productivity suite?	No
List the available mechanisms through which an external authentication store may be integrated (to enable single sign-on) (example: OpenID, LDAP, oAuth2)	oAuth 1