THE JVR AFRICA GROUP

Data Security Policy

June 2021

JVR Africa Group Data Security Policy

The JVR Africa Group respects, values, and protects all personal data collected through in person and electronic commerce practices, with the highest level of security. We agree to use such information for the purposes outlined when collected and to hold such information within the strictest confidence as is prescribed by the HPCSA (Health Professions Council of South Africa), the South African POPIA (Protection of Personal Information Act), and the international GDPR (General Data Protection Regulation) as it is relevant and aligned to local legislation and doing business across borders. This applies to both online and offline information that are collected and used in the course of running our businesses, delivering our services, and through the activities in which we are involved.

Physical Security

The data centre facilities where our servers are hosted are secure and access controlled. All equipment and servers are located in secure locked cabinets within biometrically controlled areas. Comprehensive perimeter and building security are in place, with 'zones within zones' for multiple levels of security. Specifically, pre-authorisation is required for access. Visitor identity is confirmed visually, with additional biometric confirmation. Service areas are physically separate from data centre areas. There is also continuous video surveillance of all zones and cabinets, and comprehensive audit logs on all access. All cabinets have unique locks, ensuring that only approved personnel have access per zone area.

Access to on-site JVR servers is controlled and strictly monitored. Only authorised personnel have keys.

Personnel

JVR conducts background and security screening for all personnel prior to qualification as administrators. Furthermore, JVR communicates its information security policies to its personnel and provides privacy and security training.

Encryption

JVR servers use Advanced Encryption Standard (AES) 128/256-bit for data-in-transit and data-at-rest encryptions to secure its data. For secure data transmission between websites, the latest Transport Layer Security (TLS 1.2) protocol is used, which works with the most current web browsers, encrypting information exchanged over a network and protecting against disclosure to third parties during transmission of data. To prevent data tampering, data-at-rest encryption is used to maintain data

integrity. This includes data transmission via email and via integration with client platforms utilising an Application Protocol Integration (API) interface.
Transactions between systems and backups are done through an encrypted connection.

Personal Information Security

Personal information, understood to be any information that identifies or could be used to identify an individual, is protected by JVR through a number of safety measures encompassing all systems and interactions where personal information is collected and stored. JVR actively monitors all secure information reserves (including but not limited to Order Management Systems (OMS), digital data, hard copy records, e-commerce platforms, and electronic platforms) to ensure that security measures are maintained at the highest level of security, meeting all regulatory and legal requirements.

Assessment Data Security

Access to data collected through online services, including but not limited to scoring services, is restricted to qualified users and requires a username and password. Registration of JVR customers or their designated *'Administrators'* is rigorous with defined qualification user levels. Identity is confirmed by a qualification form, which is a binding test user agreement coupled with a review of qualifications and certification.
After a person has completed registration and indicated consent, JVR will, as a matter of policy, keep on file a record of:

1. The products and services the person has purchased
2. The person's certification and qualification status
3. The person's contact information
4. Any aggregate depersonalised information including test data, indefinitely, unless otherwise stipulated or instructed.

Please note that once depersonalised, any test results or related data will no longer be considered personal information and will remain an anonymous record with no bearing or impact on the individual. In this state, it will no longer be considered a record associated with any one individual and will not be subject to regulations related to personal information and the rights of an individual.

Data Storage

All JVR data (including administrators and test user information, test data, including responses to test items and report text) are stored in an industry standard secure database. Access to this data is strictly controlled by JVR through its qualified administrators. To further protect the data transmitted to JVR electronically for assessment or other services, JVR's online scoring services encrypt access passwords, which means that identifiable data is made accessible only to the customer or their designated administrator. The test data is stored in secure servers hosted in access-controlled data centres.

Data Retention

JVR holds any aggregate depersonalised information, including test data, indefinitely. Personalised test data is kept as per HPCSA requirements and within this time period a report can be regenerated by the appropriately qualified and certified user through their online account.

Unauthorised Access

In the event that JVR becomes aware of a security breach, JVR will promptly investigate the matter and notify the applicable parties. An investigation will be conducted without delay, consistent with:

1. Legitimate requirements of law enforcement and the Privacy Commissioner's office
2. Measures necessary to determine the scope of the breach
3. Efforts to identify the individuals affected
4. Steps to identify the cause of breach, and
5. Urgent, yet reasonable restoration of the integrity of our secure server.

Risk Assessment

Formal information risk analyses are carried out for critical systems and environments as part of business continuity initiatives and are reviewed regularly. The evaluation of each threat takes into account its business impact, likelihood of occurrence, and what options are available to eliminate or mitigate the identified risk. JVR is committed to maintaining a low-risk threshold and takes active steps to proactively mitigate risk through extensive planning and implementation of improved measures.

Disaster Recovery

JVR maintains current disaster recovery plans which address data results, personal information, and online services to ensure minimal impact to customers using applications, while maintaining the strictest level of security throughout. For further information regarding compliance specific to these elements, please contact the information officer at JVR at +27 (0) 11 781 3705/6/7 during office hours or send an email to: informationofficer@jvrafrica.co.za.

Qualification

Eligibility to purchase restricted products requires the completion of a qualification form which requires the validation of identity, credentials, and other information as deemed necessary. Certification results are retained by JVR but are not disclosed to a third party, including an employer, without prior written consent.

Consent to Data Use

All personal information is kept strictly anonymous with all data adhering to the record retention security protocols and standards. The collection of personal information is limited to what has been identified as necessary for the purpose. Consent for the collection of data is obtained as follows:

- Expressed and implied consent are given at the time an assessment is administered or a service is provided. Qualified and professional persons overseeing the assessment, offering the certification or other training, and/or facilitation, or providing the consulting process/intervention are bound by nationally and internationally recognised professional and ethical rules.
- Express consent is provided for the collection of data for qualified research and e-commerce activities.

Third Party Access to Data

Personal data of any kind related to clients/customers or their own clients are never sold to any third parties. JVR holds all information collected in strict confidence, taking active measures to protect any and all data, and is committed to continuously enhancing its overall security through ongoing improvements and constant monitoring. Internal administrators employed by JVR are able to audit records accessed within the system as a mechanism of monitoring and breach control. Any service providers with access to systems as part of the provision of support services are bound by contractual and non-disclosure agreements.

Contact Information

Should you have any questions or concerns regarding this policy, please contact the JVR Africa Group Information Officer at +27 (0) 11 781 3705/6/7 during office hours or send an email to: informationofficer@jvrafrica.co.za

Security and Privacy

Please note that the JVR data security protocols are formulated in our Security and Privacy Policies available on the JVR systems site. This document should be read in conjunction with these and all the other JVR Terms of Business Policies available on this site.