	INFORMATION SECURITY, DATA PROTECTION (POPI ACT) AND CYBER SECURITY STATEMENT - EXTERNAL
THE PARTIES	ENTERED INTO BY AND BETWEEN: **ID VERIFICATION SYSTEMS CLOSE CORPORATION** **(REGISTRATION NUMBER 2006/169367/23)** ("IVS") and **THE CLIENT / USER**
NOTICE	© Copyright subsists in this material in terms of the Copyright Act No 98 of 1978. No part or portion of this document may be reproduced or transmitted in any form or by any means electronic or mechanical, including photocopying, scanning, recording or by any information in storage and retrieval system without the written permission of Ryan Attorneys.

POPI ACT AND DATA PROTECTION

Note: The obligations contained herein shall survive the termination hereof or any other agreement between IVS and yourselves, and as prescribed in terms of the POPI Act.

Any breach of any of the provisions contained herein shall be regarded as a material breach of your obligations to IVS.

By accessing an/or clicking on this link and/or by opening this document and/or dealing with IVS you indemnify IVS against any loss incurred or damages suffered for any breach of this agreement on your side.

The latter applies vice versa to IVS.

It is specifically recorded that, in consequence of the Services that you render to IVS and/or Services IVS renders to you and/or based on the business relationship between IVS and yourselves, and due to the stringent terms of the new POPI Act, act 4 of 2013, it is inevitable that you will collect, store and process Personal Information (as defined in the Protection of Personal Information Act) belonging to IVS and/or third parties for which IVS is responsible for the protection of such data and Personal Information. This applies vice versa.

By clicking and/or accessing an IVS link and/or sharing and/or obtaining information from IVS, both parties confirm, accept and irrevocably warrant that they will:

1. Ensure that they are fully aware of the terms and regulations of the Protection of Personal Information Act (POPI Act), Act 4 of 2013 and that it will be read in conjunction with this agreement.

2. Not divulge or otherwise make available the Personal Information to any third party other than authorized staff or subcontractors who require access to such Personal Information strictly in order to carry out their obligations pursuant to your obligations to the other party.

3. Ensure that your employees, agents, subsidiaries, representatives, subcontractors and/or any other persons that have access to the Personal Information are bound by appropriate and legally binding confidentiality and/or non-disclosure obligations in respect to the Personal Information and as provided for in the POPI Act.

4. Comply with the provisions of the prevailing security, privacy and data protection legislation and/or regulations governing the collection, use, storage and processing of Personal Information as defined in relevant legislation and only act on the explicit written instructions of either party in collecting, storing, processing and utilisation of the relevant Personal Information.

5. Not divulge, use, store and/or process Personal Information for any purpose other than to perform their respective obligations to the other party, and to ensure that such processing will not place either party in breach of any privacy and data protection laws or related requirements, more specifically the POPI Act.

6. Take appropriate, reasonable, technical and organisational measures to ensure that the integrity and confidentiality of the Personal Information in your possession, or under your control, is secure and that such Personal Information is protected against accidental loss, destruction, damage, unlawful access and/or processing.

7. Immediately notify the other party in the event of possible infringements of the applicable data protection legislation, the terms of this agreement or other irregularities by either party, their staff or any other party acting on your behalf in relation to the Personal Information.

8. Return, destroy and/or store in an appropriate manner the Personal Information once it is no longer required for the purpose of performing your obligations to the other party or any directly related purpose; and fully indemnify and hold the other party, its affiliates, associates, subsidiaries and their respective staff, successors, cessionary and assigns, harmless from all and any losses, costs (including but not limited to legal costs on an attorney and own client scale), expenses and/or damage (including but not limited to consequential losses and damages) as well as penalties and fines arising out of, or relating to any non-compliance with the provisions of this agreement and any relevant data protection legislation by either party, or any other party who received Personal Information from the other.

9. Only transfer Personal Information across country borders with either party's prior written consent. In this regard, you shall ensure that any such transfer of any Personal Information across country borders complies with applicable laws and related legislation. It is specifically recorded that IVS will store and/or transfer Personal Information on a daily basis across country borders, due to the type Service that IVS is rendering to you. By undersigning this you give IVS consent to transfer same and acknowledge that you are aware of the fact that IVS will transfer Personal Information across country borders.

CYBER SECURITY POLICY AND STRATEGY

10. **Purpose**

The purpose of IVS' Cyber Security Policy is to protect the confidentiality, integrity, and availability of all IVS and Client information, third parties linked to IVS, systems, and digital assets. As an IT (hosting and/or developer company), we recognise that cyber security is fundamental to operational continuity, client trust, and regulatory compliance.

11. **Scope**

This policy applies to:

- All employees, contractors, consultants, and third parties linked to IVS
- All IT systems, networks, software, cloud services, and data
- All devices used to access company systems (company-owned or personal)

12. **Security Principles**

For the Client we commit to:

- Implementing industry best practices for cyber security
- Complying with all applicable data protection and privacy laws
- Applying the principle of least privilege for system access
- Maintaining secure system configurations and patch management
- Encrypting sensitive data in transit and at rest
- Performing regular backups and recovery testing
- Monitoring systems for unauthorized access or suspicious activity

13. **Ensure Access Control**

- Note that access to systems is role-based and authorised by management.
- Multi-factor authentication (MFA) is enforced where possible.
- User access rights are reviewed periodically.
- Accounts are disabled immediately upon termination of employment.

14. **Data Protection**

- Sensitive and client data will be handled securely at all times.
- Confidential information will not be shared without authorisation.
- Secure file transfer methods will be used for external communication.

15. **Incident Management**

- All suspected security incidents must be reported immediately to management or the designated IT security officer.
- Incidents will be logged, investigated, and resolved promptly.
- Clients will be notified in accordance with contractual and legal obligations.

16. **Employee Responsibilities**

All personnel are required to:

- Complete periodic threat awareness training
- Use strong passwords and maintain password confidentiality
- Avoid phishing, malware, and social engineering risks
- Report any security weaknesses immediately

Failure to comply with this policy may result in disciplinary action for IVS staff.

17. **Policy Review**

This policy will be reviewed annually or upon significant changes in technology, risk, or legislation.

CYBER SECURITY STATEMENT

At IVS, cyber security is a core business priority. We are committed to protecting our clients', service provider's and/or related third parties' data, systems, and digital assets through proactive risk management, secure infrastructure, continuous monitoring, and staff awareness.

We maintain appropriate technical and organisational measures to safeguard information against unauthorised access, alteration, disclosure, or destruction. Our security framework is aligned with recognised industry standards and best practices.

Should you have an concerns in as far as it relates to this document please note that the duly appointed Information Officer is Ms. Antoinette van Jaarsveld who can be contacted at antoinette@idvsystems.co.za.