

# POPI COMPLIANCE: WEBSITE PRIVACY POLICY

## 1. SCHEDULE

1.1 The Company (Organisation) RISK TRAIN (PTY) LTD

1.2 Registration number 2025/431915/07

1.3 VAT registration number N/A

1.4 Physical address UNIT 28 PILKINGTON BUSINESS PARK, CNR JOHAN LE ROUX AND MORRIS ROAD, MEYERTON

1.5 Email address INFO@RISKTRAIN.CO.ZA

1.6 Website address WWW.RISKTRAIN.CO.ZA

## 2. COMMITMENT TO YOUR PRIVACY

### 2.1

Welcome to the website of Risk Train (Pty) Ltd (“Risk Train”, “the Company”, “we”, “us” or “our”), including the website located at [www.risktrain.co.za](http://www.risktrain.co.za) and any associated online platforms, learner management systems or digital training portals (“Website”).

Risk Train is committed to protecting the privacy and confidentiality of all personal information entrusted to it by learners, clients, employees, contractors, assessors, moderators, suppliers, visitors and users of the Website. Risk Train recognises that maintaining the trust and confidence of stakeholders requires transparency, accountability and responsible management of personal information.

Initial

This Privacy Policy (“Policy”) forms part of and must be read together with Risk Train’s Terms and Conditions of Use, PAIA Manual, POPIA Compliance Framework and any other applicable policies published by Risk Train.

## **2.2**

In the ordinary course of its business operations, including the provision of training, assessment, moderation, certification, consulting and related services, Risk Train may collect, process, store, use and disclose Personal Information. Such processing may include information relating to learners, employees, clients, service providers, facilitators, assessors, moderators and other stakeholders.

Risk Train undertakes to process all Personal Information lawfully, reasonably and transparently in accordance with the Protection of Personal Information Act 4 of 2013 (“POPIA”), the Promotion of Access to Information Act 2 of 2000 (“PAIA”) and other applicable South African legislation. Personal Information will only be processed where:

- consent has been obtained where required by law;
- processing is necessary to fulfil contractual or legal obligations;
- processing is necessary for legitimate operational, training, accreditation or certification purposes; or
- processing is otherwise permitted in terms of applicable legislation.

## **2.3**

This Policy explains how Risk Train collects, records, stores, uses, shares, safeguards and destroys Personal Information in the course of conducting its business activities. The Policy further explains the rights of data subjects in relation to their Personal Information and the measures implemented by Risk Train to ensure the confidentiality, integrity and security of such information.

# **3. DEFINITIONS**

## **3.1**

In this Privacy Policy (“Policy”), unless the context indicates otherwise, the following words and expressions shall bear the meanings assigned to them below. Words importing the singular shall include the plural and vice versa, words importing any gender shall include the other genders, and references to natural persons shall include juristic persons where applicable.

### **3.1.1 “Applicable Legislation”**

Means all legislation, regulations, codes of conduct, standards and legal requirements applicable to Risk Train and the processing of Personal Information in the Republic of South Africa, including but not limited to:

- the Protection of Personal Information Act 4 of 2013 (“POPIA”);
- the Promotion of Access to Information Act 2 of 2000 (“PAIA”);
- the Electronic Communications and Transactions Act 25 of 2002 (“ECTA”);
- the Consumer Protection Act 68 of 2008 (“CPA”);
- the Occupational Health and Safety Act 85 of 1993 (“OHS Act”); and
- any applicable QCTO, SETA, SAQA or regulatory requirements.

Initial

### **3.1.2 “Biometric Information”**

Means personal information relating to the physical, physiological or behavioural identification of a person, including fingerprints, facial recognition, photographs, video recordings, voice recordings or any other identifiable biometric identifier.

### **3.1.3 “Data Subject”**

Means the natural person or juristic person to whom Personal Information relates, including but not limited to learners, employees, clients, contractors, suppliers, assessors, moderators, facilitators, visitors and users of the Website.

### **3.1.4 “Information Officer”**

Means the duly appointed Information Officer of Risk Train as contemplated in POPIA and PAIA, including any duly authorised Deputy Information Officer.

### **3.1.5 “Operator”**

Means a third party who processes Personal Information on behalf of Risk Train in terms of a contract or mandate, including cloud service providers, learning management system providers, IT service providers, payroll administrators or external assessment platforms.

### **3.1.6 “Personal Information”**

Means information relating to an identifiable, living natural person and, where applicable, an identifiable existing juristic person, as defined in POPIA, including but not limited to:

- names and surnames;
- identity or passport numbers;
- date of birth;
- contact details;
- residential and postal addresses;
- email addresses;
- employment details;
- educational, training and assessment records;
- medical or health-related information;
- biometric information;
- photographs and video recordings;
- financial information;
- race, gender, nationality and language;
- online identifiers and IP addresses;
- correspondence and communications; and
- any other information recognised as personal information in terms of Applicable Legislation.

### **3.1.7 “Processing”**

Means any operation or activity concerning Personal Information, whether automated or not, including the collection, receipt, recording, organisation, storage, updating, modification, retrieval, use, dissemination, distribution, transfer, merging, restriction, deletion or destruction of Personal Information.

### **3.1.8 “Responsible Party”**

Means Risk Train (Pty) Ltd, being the entity that determines the purpose of and means for processing Personal Information.

### **3.1.9 “Risk Train”, “the Company”, “we”, “us” or “our”**

Means Risk Train (Pty) Ltd, its divisions, subsidiaries, affiliates, authorised representatives, employees, contractors and operators acting within the scope of their duties and authority.

### **3.1.10 “User”, “you”, “your” or “yourself”**

Means any person who accesses, browses, uses, interacts with or submits information through the Website or makes use of any services offered by Risk Train, whether such use is free of charge, contractual, commercial, educational or otherwise.

### **3.1.11 “Website”**

Means the official Risk Train website located at [www.risktrain.co.za](http://www.risktrain.co.za), including any related learner management systems, online training portals, electronic communication platforms, mobile applications and digital systems operated or controlled by Risk Train.

## **3.2**

Unless the contrary intention clearly appears from the context:

- any term specifically defined in POPIA, PAIA or other Applicable Legislation shall bear the meaning assigned to it in such legislation;
- headings are included for convenience only and shall not affect the interpretation of this Policy; and
- references to legislation shall include any amendments, re-enactments or substitutions thereof from time to time.

## **4. COLLECTION AND PROCESSING OF PERSONAL INFORMATION**

### **4.1**

Risk Train (Pty) Ltd (“Risk Train”) collects and processes Personal Information in the ordinary course of conducting its business operations, including but not limited to:

- the provision of training, assessment, moderation and certification services;
- QCTO, SETA and SAQA compliance and reporting obligations;
- learner registration and administration;
- employment and human resource administration;
- occupational health and safety management;
- client relationship management;
- supplier and contractor management;
- marketing and communication activities;

Initial

- access control and security management;
- operation of its Website, learner management systems (“LMS”), digital platforms and electronic communication systems; and
- compliance with legal, regulatory and contractual obligations.

## 4.2

The categories of Personal Information processed by Risk Train may include, but are not limited to:

- names and surnames;
- identity numbers, passport numbers and registration details;
- contact information;
- residential and postal addresses;
- employment and qualification information;
- learner enrolment records;
- assessment results and moderation records;
- portfolios of evidence;
- attendance registers;
- certification and competency records;
- photographs, CCTV footage and video recordings;
- medical or fitness declarations where operationally required;
- biometric information where lawfully authorised;
- financial and banking information;
- online identifiers, website usage data and IP addresses; and
- correspondence, communications and contractual records.

## 4.3

Risk Train collects Personal Information directly from data subjects, through authorised third parties, through contractual engagements, through training and assessment processes, through the use of the Website and electronic systems, and through lawful operational and regulatory processes.

## 4.4

Risk Train undertakes to process all Personal Information:

- lawfully, reasonably and transparently;
- only for specific, explicitly defined and legitimate purposes;
- in a manner that does not unlawfully infringe the privacy rights of any data subject;
- in accordance with the provisions of POPIA and all Applicable Legislation;
- subject to appropriate technical and organisational security safeguards; and
- only for as long as reasonably necessary to fulfil the purpose for which the information was collected or as required by law.

## 4.5

Risk Train may process Personal Information where:

- the data subject has provided consent;
- processing is necessary to perform contractual obligations;
- processing is necessary to comply with legal or regulatory obligations;
- processing is necessary for legitimate operational, accreditation, certification or safety purposes; or
- processing is otherwise permitted in terms of Applicable Legislation.

## 4.6

Risk Train is committed to ensuring that Personal Information is only used for legitimate business, educational, operational, safety, accreditation and compliance purposes directly related to the lawful activities of the organisation.

## 4.7

Where required by law or operational necessity, Risk Train may disclose Personal Information to:

- QCTO;
- SETAs;
- SAQA;
- regulatory authorities;
- accreditation bodies;
- external moderators and verifiers;
- professional advisors;
- authorised service providers and operators;
- law enforcement agencies; or
- any other party where disclosure is legally required or permitted.

## 4.8

Risk Train will take all reasonable steps to ensure that Personal Information processed by or on behalf of the organisation remains accurate, complete, relevant, secure and up to date.

# 5. CONSENT TO THE PROCESSING OF PERSONAL INFORMATION

## 5.1

Risk Train (Pty) Ltd (“Risk Train”) respects the privacy rights of all data subjects and undertakes to process Personal Information lawfully, reasonably and transparently in accordance with the Protection of Personal Information Act 4 of 2013 (“POPIA”) and all Applicable Legislation.

## 5.2

Risk Train will, where required by law, obtain the voluntary, specific and informed consent of the relevant data subject prior to collecting, processing, using, storing or disclosing Personal Information.

Initial

### 5.3

By providing Personal Information to Risk Train, using the Website, enrolling for training, submitting forms, entering into agreements, attending training programmes, participating in assessments or otherwise engaging with Risk Train's services, the data subject acknowledges and agrees that Risk Train may process such Personal Information for legitimate operational, educational, accreditation, certification, safety, contractual and compliance-related purposes.

### 5.4

Risk Train may process Personal Information without consent where such processing:

- is required or permitted by law;
- is necessary to comply with legal or regulatory obligations;
- is necessary for the conclusion or performance of a contract;
- protects the legitimate interests of the data subject;
- is necessary for pursuing the legitimate interests of Risk Train or a third party;
- is required for QCTO, SETA, SAQA or regulatory reporting purposes; or
- is otherwise authorised in terms of POPIA or Applicable Legislation.

### 5.5

Where consent is relied upon as the lawful basis for processing, the data subject may withdraw such consent at any time by written notice to Risk Train, provided that:

- the withdrawal of consent shall not affect the lawfulness of any processing conducted prior to such withdrawal; and
- withdrawal of consent may limit Risk Train's ability to provide certain services, training, assessments, certifications or Website functionality.

### 5.6

Risk Train shall take all reasonable steps to ensure that data subjects are adequately informed regarding:

- the nature and purpose of the processing;
- the categories of Personal Information being collected;
- the recipients or categories of recipients of such information;
- the consequences of failing to provide required information; and
- the rights available to data subjects in terms of POPIA.

### 5.7

Where required by law, Risk Train shall obtain separate or additional consent for:

- direct electronic marketing communications;
- the processing of special personal information;
- the processing of children's personal information;
- biometric processing activities; or
- the use of photographs, videos or training recordings for promotional or educational purposes.

Initial

# **6. USE, DISCLOSURE AND CROSS-BORDER TRANSFER OF PERSONAL INFORMATION**

## **6.1**

Risk Train (Pty) Ltd (“Risk Train”) operates its Website, digital platforms, learner management systems and business operations in accordance with the Constitution of the Republic of South Africa, the Protection of Personal Information Act 4 of 2013 (“POPIA”), the Promotion of Access to Information Act 2 of 2000 (“PAIA”) and all other Applicable Legislation.

Risk Train recognises the constitutional and statutory rights of data subjects to privacy and is committed to ensuring that all Personal Information is processed lawfully, reasonably, transparently and securely.

## **6.2**

Risk Train may use Personal Information for legitimate business, operational, educational, accreditation, certification, safety and compliance purposes, including but not limited to:

- learner registration and administration;
- training delivery and assessment activities;
- moderation and certification processes;
- QCTO, SETA and SAQA reporting;
- occupational health and safety compliance;
- contractual and client management;
- communication and customer support;
- website and system administration;
- quality assurance and auditing;
- legal and regulatory compliance; and
- security, fraud prevention and risk management.

## **6.3**

Risk Train may disclose Personal Information where reasonably necessary and lawfully permitted to:

- QCTO;
- SETAs;
- SAQA;
- accreditation bodies;
- external moderators, assessors and verifiers;
- professional advisors, auditors and legal representatives;
- authorised operators and service providers;
- payment processors and financial institutions;
- regulatory or governmental authorities;
- law enforcement agencies; or

- any other party where disclosure is required or permitted by law.

## **6.4**

Risk Train shall take all reasonable steps to ensure that any third party receiving Personal Information:

- is subject to appropriate confidentiality obligations;
- processes such information only for authorised purposes;
- implements appropriate technical and organisational security safeguards; and
- complies with the requirements of POPIA and other Applicable Legislation where applicable.

## **6.5**

Risk Train may transfer, store or process Personal Information outside the Republic of South Africa, including through the use of:

- cloud-based platforms;
- electronic communication systems;
- learning management systems;
- website hosting providers;
- backup and disaster recovery systems; and
- international software or service providers.

Such cross-border transfers may occur where systems or infrastructure utilised by Risk Train are hosted in foreign jurisdictions.

## **6.6**

Where Personal Information is transferred outside South Africa, Risk Train will take all reasonable and appropriate steps to ensure that:

- the recipient is subject to laws, binding agreements or security measures that provide an adequate level of protection substantially similar to that required under POPIA;
- the transfer is necessary for the performance of contractual obligations;
- the transfer is required for lawful operational or regulatory purposes; or
- the data subject has consented to the transfer where required by law.

## **6.7**

Risk Train shall not sell, trade or unlawfully disclose Personal Information to third parties for commercial exploitation or unrelated marketing purposes.

## **6.8**

Risk Train reserves the right to disclose Personal Information where such disclosure:

- is required by a court order, subpoena or lawful governmental request;
- is necessary to protect the rights, property or safety of Risk Train, its employees, learners, clients or the public;
- is necessary to investigate fraud, misconduct, security incidents or unlawful activities; or
- is otherwise authorised or required by Applicable Legislation.

Initial

# **7. RETENTION, STORAGE AND DESTRUCTION OF PERSONAL INFORMATION**

## **7.1**

Risk Train (Pty) Ltd (“Risk Train”) shall retain Personal Information only for as long as is reasonably necessary to fulfil the purpose for which such information was collected or processed, unless:

- a longer retention period is required or permitted by law;
- retention is necessary for lawful operational, accreditation, certification or historical record purposes;
- retention is required for the establishment, exercise or defence of legal rights;
- retention is required in terms of contractual obligations; or
- the data subject has consented to a longer retention period.

## **7.2**

Risk Train retains Personal Information in accordance with:

- the Protection of Personal Information Act 4 of 2013 (“POPIA”);
- the Promotion of Access to Information Act 2 of 2000 (“PAIA”);
- the Companies Act 71 of 2008;
- the Income Tax Act 58 of 1962;
- the Value Added Tax Act 89 of 1991;
- the Basic Conditions of Employment Act 75 of 1997;
- the Labour Relations Act 66 of 1995;
- the Occupational Health and Safety Act 85 of 1993;
- QCTO, SETA and SAQA requirements;
- applicable accreditation and certification standards; and
- any other Applicable Legislation or regulatory requirements.

## **7.3**

Personal Information may be retained in both physical and electronic formats, including:

- hard copy files;
- learner portfolios of evidence;
- assessment and moderation records;
- training attendance registers;
- digital databases;
- cloud-based systems;
- email systems;
- learning management systems (“LMS”);
- backup and disaster recovery systems; and

Initial

- CCTV, photographic and video archives where applicable.

## 7.4

Risk Train may retain records relating to:

- learner enrolment and certification;
- assessments and moderation;
- statements of results;
- recognition of prior learning (“RPL”);
- training attendance;
- employee and contractor records;
- financial and taxation records;
- health and safety incidents;
- legal disputes and investigations;
- client and supplier contracts; and
- regulatory and accreditation compliance activities.

## 7.5

Without limiting the generality of the above, Risk Train may retain certain categories of records for the following indicative periods, unless otherwise required by law:

- learner records and assessment documentation: minimum of five (5) years;
- moderation reports and certification records: minimum of five (5) years;
- financial and taxation records: minimum of five (5) years;
- employment and payroll records: as prescribed by labour legislation;
- health and safety incident records: as prescribed by the Occupational Health and Safety Act and related regulations;
- accreditation and compliance records: for the duration required by the applicable authority or accreditation body;
- CCTV and access-control footage: for a reasonable operational and security period unless required for investigation purposes.

## 7.6

Risk Train shall take all reasonable technical and organisational measures to ensure that retained Personal Information:

- remains accurate, complete and up to date where reasonably practicable;
- is protected against loss, unauthorised access, misuse, disclosure or destruction;
- is accessible only to authorised persons with legitimate business reasons for access; and
- is securely archived, backed up and recoverable where operationally necessary.

## 7.7

Once Personal Information is no longer required for the purpose for which it was collected and no lawful basis for continued retention exists, Risk Train shall take reasonable steps to permanently destroy, de-identify or anonymise such information in a secure manner designed to prevent reconstruction or unlawful access.

## **7.8**

The destruction or disposal of records containing Personal Information may include:

- secure shredding of physical documents;
- permanent deletion of electronic records;
- destruction of storage media;
- anonymisation or de-identification processes; or
- secure disposal through authorised service providers bound by confidentiality obligations.

## **7.9**

Where Personal Information is retained for historical, statistical, research, legal, audit or accreditation purposes, Risk Train shall continue to apply appropriate safeguards to protect such information in accordance with POPIA and Applicable Legislation.

## **7.10**

Data subjects may request access to, correction of, deletion of or objection to the processing of their Personal Information in accordance with POPIA, PAIA and Risk Train's applicable policies and procedures, subject to any legal or operational limitations applicable to such requests.

# **8. YOUR RIGHTS IN RELATION TO PERSONAL INFORMATION**

## **8.1**

Risk Train (Pty) Ltd ("Risk Train") recognises and respects the rights of all data subjects in relation to their Personal Information as provided for in the Protection of Personal Information Act 4 of 2013 ("POPIA"), the Promotion of Access to Information Act 2 of 2000 ("PAIA") and other Applicable Legislation.

## **8.2**

Subject to applicable legal limitations and verification requirements, every data subject has the right to:

- be informed whether Risk Train holds Personal Information relating to them;
- request access to Personal Information held by Risk Train;
- request correction, updating or rectification of inaccurate, incomplete, misleading or outdated Personal Information;
- object to the processing of Personal Information under certain circumstances;
- request deletion, destruction or de-identification of Personal Information where such information is no longer required for lawful purposes;
- withdraw consent where processing is based on consent;
- lodge a complaint with the Information Regulator; and
- institute civil proceedings where appropriate.

Initial

### 8.3

A data subject may, at any reasonable time and subject to compliance with applicable procedures, contact Risk Train to:

- confirm whether Risk Train processes or holds Personal Information relating to them;
- obtain access to records or categories of Personal Information relating to them;
- request details regarding the source of the Personal Information where reasonably available;
- request details regarding third parties or categories of third parties who have had access to such Personal Information where legally permissible;
- request correction or updating of Personal Information;
- object to the processing of Personal Information;
- request restriction of processing activities in certain circumstances; or
- request the deletion or destruction of Personal Information.

### 8.4

Requests for access to Personal Information or records may be made in accordance with:

- Risk Train's PAIA Manual;
- prescribed PAIA or POPIA forms where applicable; and
- the procedures communicated by the Information Officer.

Certain requests may be subject to the payment of prescribed fees in terms of PAIA and applicable regulations.

### 8.5

Risk Train reserves the right to take reasonable steps to verify the identity of any person making a request relating to Personal Information in order to:

- prevent unauthorised access;
- protect confidential information;
- safeguard the privacy rights of third parties; and
- ensure compliance with legal obligations.

Such verification may include requests for:

- proof of identity;
- proof of authority;
- written mandates;
- supporting documentation; or
- additional information reasonably required to process the request.

### 8.6

Risk Train may refuse, limit or defer access to Personal Information or records where:

- disclosure would unreasonably infringe the privacy rights of another person;

Initial

- disclosure would reveal confidential or commercially sensitive information;
- the records are legally privileged;
- disclosure is prohibited by law;
- the request is manifestly unfounded, excessive or vexatious; or
- grounds for refusal exist in terms of PAIA, POPIA or Applicable Legislation.

Where access is refused or limited, Risk Train shall provide written reasons for such decision unless prohibited by law.

## **8.7**

If a data subject believes that Personal Information held by Risk Train is:

- inaccurate;
- irrelevant;
- excessive;
- outdated;
- incomplete;
- misleading;
- unlawfully obtained; or
- unlawfully retained,

the data subject may request that such information be corrected, updated, restricted, destroyed, deleted or de-identified, subject to any legal, operational, accreditation or regulatory obligations requiring retention of the information.

## **8.8**

Risk Train may decline requests for deletion or destruction of Personal Information where retention is required:

- by law;
- for QCTO, SETA or SAQA compliance;
- for accreditation or certification purposes;
- for legal proceedings or investigations;
- for contractual obligations;
- for historical or audit purposes; or
- for legitimate operational requirements.

## **8.9**

Where processing of Personal Information is based on consent, a data subject may withdraw such consent at any time by written notice to Risk Train. Withdrawal of consent shall not:

- affect the lawfulness of processing undertaken prior to withdrawal; or
- affect processing conducted on another lawful basis permitted under POPIA.

## **8.10**

Initial

Data subjects acknowledge that restricting or withdrawing consent to the processing of certain Personal Information may:

- limit Risk Train’s ability to provide services;
- affect learner registration, assessment or certification processes;
- prevent access to training programmes or digital platforms;
- affect compliance with legal or accreditation obligations; or
- otherwise impact the quality, functionality or availability of services.

## **8.11**

Any complaints regarding the processing of Personal Information may be directed to Risk Train’s Information Officer using the contact details contained in this Policy. Data subjects also have the right to lodge complaints with the Information Regulator of South Africa.

## **8.12**

Risk Train undertakes to handle all requests and complaints relating to Personal Information in a fair, lawful, transparent and reasonable manner and within the time periods prescribed by Applicable Legislation.

# **9. INFORMATION SECURITY AND SAFEGUARDS**

## **9.1**

Risk Train (Pty) Ltd (“Risk Train”) recognises the importance of protecting Personal Information against loss, misuse, unauthorised access, disclosure, alteration, destruction or any other unlawful processing activity. Risk Train accordingly undertakes to implement and maintain appropriate, reasonable and commercially acceptable technical, physical, electronic and organisational safeguards to protect the confidentiality, integrity and availability of Personal Information under its possession or control.

## **9.2**

Risk Train maintains an integrated information security framework aligned with:

- the Protection of Personal Information Act 4 of 2013 (“POPIA”);
- generally accepted information security principles and industry practices;
- operational risk management requirements;
- QCTO, SETA and accreditation obligations where applicable; and
- the legitimate operational requirements of the organisation.

## **9.3**

Risk Train may implement and maintain security measures including, but not limited to:

- firewall and network protection systems;
- password protection and authentication controls;
- encryption technologies;
- antivirus and anti-malware systems;
- endpoint protection systems;

- role-based access controls;
- secure cloud and backup infrastructure;
- email filtering and cyber-security protections;
- restricted physical access controls;
- CCTV and premises security systems;
- secure destruction and disposal procedures;
- audit trails and activity monitoring;
- disaster recovery and business continuity measures; and
- controlled access to learner, employee and client records.

## 9.4

Access to Personal Information is restricted to authorised persons who require such access for legitimate operational, educational, contractual, accreditation, compliance or legal purposes. All employees, facilitators, assessors, moderators, contractors, operators, consultants and service providers who may have access to Personal Information may be required to:

- comply with Risk Train's information security policies and procedures;
- adhere to confidentiality obligations;
- process Personal Information only for authorised purposes; and
- implement appropriate safeguards to protect such information.

## 9.5

Risk Train shall take reasonable steps to ensure that third-party operators, service providers and technology platforms processing Personal Information on behalf of Risk Train:

- provide sufficient security guarantees;
- implement appropriate technical and organisational security measures;
- comply with POPIA and Applicable Legislation where applicable; and
- are contractually bound to maintain confidentiality and security.

## 9.6

Risk Train continuously identifies, assesses and monitors reasonably foreseeable internal and external risks to Personal Information in its possession or under its control, including risks relating to:

- cyber threats;
- malware and ransomware attacks;
- unauthorised access;
- data breaches;
- human error;
- theft or loss of devices;
- system failures;
- accidental disclosure;

- operational disruptions; and
- unlawful processing activities.

## 9.7

Risk Train undertakes to:

- establish and maintain appropriate safeguards against identified risks;
- regularly review and test security controls and procedures;
- monitor systems and access activities where reasonably necessary;
- update security measures in response to evolving operational, technological and cyber-security risks; and
- take reasonable corrective action where vulnerabilities or deficiencies are identified.

## 9.8

While Risk Train takes all reasonable and appropriate precautions to safeguard Personal Information, no method of transmission, storage or electronic processing can be guaranteed to be completely secure or immune from unauthorised access, cyberattack, system failure or human error. Accordingly:

- Risk Train does not warrant or guarantee absolute security of any Personal Information;
- data subjects provide information and utilise electronic systems at their own risk to the extent permitted by law; and
- Risk Train shall not be liable for any loss, damage or unauthorised access arising from circumstances beyond its reasonable control, provided that Risk Train has complied with its legal obligations relating to security safeguards.

## 9.9

In the event of any actual or suspected security compromise involving Personal Information, Risk Train may:

- investigate the incident;
- take reasonable steps to contain and mitigate the effects of the compromise;
- notify affected persons and/or the Information Regulator where required by law; and
- implement corrective measures to reduce the likelihood of recurrence.

## 9.10

Risk Train reserves the right to:

- monitor and regulate the use of its information systems, digital platforms, learner management systems and electronic communications infrastructure;
- restrict or terminate access where security risks are identified; and
- implement additional security measures at any time in the interests of operational integrity, regulatory compliance, cyber-security or protection of Personal Information.

# 10. COOKIES AND WEBSITE ANALYTICS

## 10.1

Risk Train (Pty) Ltd (“Risk Train”) may make limited use of cookies, analytics tools and similar technologies on its Website and related digital platforms in order to:

- ensure the proper operation and security of the Website;
- improve Website functionality and user experience;
- analyse Website traffic and usage trends;
- maintain user sessions where applicable;
- improve Website performance and content delivery; and
- support legitimate operational, security and administrative functions.

## **10.2**

Cookies are small text files that may be stored on a user’s device or internet browser when visiting a website. Cookies generally assist websites to recognise user devices, remember preferences, improve functionality and collect general usage information.

## **10.3**

Risk Train may utilise:

- session cookies, which are temporary and expire automatically when a browser session ends;
- essential cookies required for basic Website functionality;
- limited analytics or performance cookies used to monitor Website performance and user interaction trends; and
- security-related cookies used to help detect malicious activity, unauthorised access attempts or system abuse.

## **10.4**

Risk Train does not intentionally use cookies to:

- unlawfully collect sensitive personal information;
- conduct intrusive behavioural profiling;
- sell personal information to third parties; or
- track users across unrelated third-party websites for unrelated advertising purposes.

## **10.5**

Information collected through cookies and analytics technologies may include:

- browser type and version;
- device type;
- operating system;
- IP address;
- pages visited;
- time spent on pages;
- referring websites;
- search terms used on the Website; and

- general Website interaction statistics.

Such information is generally collected in aggregated or anonymised form and is primarily used for operational, analytical, security and performance purposes.

## **10.6**

Certain third-party service providers utilised by Risk Train, including website hosting providers, analytics services, embedded content providers or learning management systems (“LMS”), may independently make use of cookies or similar technologies. Risk Train does not control the cookie practices of independent third-party platforms and users are encouraged to review the applicable privacy and cookie policies of such third parties where relevant.

## **10.7**

Users may configure their internet browsers to:

- refuse cookies;
- notify them when cookies are being used; or
- delete previously stored cookies.

However, disabling certain cookies may affect the functionality, availability or performance of portions of the Website or related systems.

## **10.8**

Risk Train reserves the right to update or modify its use of cookies, analytics technologies or digital tracking tools from time to time in accordance with operational requirements, technological developments and applicable legal obligations.

## **10.9**

By continuing to use the Website, users acknowledge and consent to the limited use of cookies and similar technologies as described in this Policy, subject to browser settings and applicable law.

# **11. THIRD-PARTY WEBSITES, EXTERNAL SERVICES AND DIRECT MARKETING**

## **11.1**

The Risk Train Website, learner management systems (“LMS”), electronic communication platforms and digital services may contain links to, integrations with, embedded content from or references to third-party websites, systems, applications or service providers (“Third-Party Platforms”).

Such Third-Party Platforms may include:

- external training or conferencing platforms;
- payment gateways;
- cloud-hosted systems;
- accreditation portals;
- social media platforms;
- analytics providers;
- document-sharing services; and

Initial

- other independently operated websites or systems.

## **11.2**

Third-Party Platforms operate independently from Risk Train and are governed by their own:

- terms and conditions;
- privacy policies;
- cookie policies;
- security practices; and
- data processing procedures.

Risk Train does not own, manage or control such Third-Party Platforms and, to the maximum extent permitted by law, does not accept responsibility or liability for:

- the availability, accuracy or reliability of such platforms;
- the content, products, services or information provided by third parties;
- the privacy or security practices of third parties;
- any loss, damage or unauthorised disclosure arising from the use of Third-Party Platforms; or
- the processing of Personal Information by independent third parties.

## **11.3**

Users who access or make use of any Third-Party Platform do so entirely at their own risk and are encouraged to review the applicable terms, privacy policies and security practices of such third parties before providing any Personal Information or making use of their services.

## **11.4**

Risk Train may from time to time communicate with learners, clients, customers or Website users regarding:

- training programmes;
- course updates;
- certification matters;
- regulatory or compliance notices;
- operational communications;
- safety information;
- service-related updates; and
- marketing or promotional material relating to products or services offered by Risk Train.

## **11.5**

Where required by law, Risk Train shall obtain the necessary consent prior to sending direct electronic marketing communications.

In accordance with POPIA, Risk Train may send direct marketing communications to:

- existing customers in relation to similar products or services previously supplied by Risk Train, subject to applicable legal requirements and opt-out rights; or

Initial

- persons who have expressly consented to receiving such communications.

## **11.6**

All direct marketing communications distributed by Risk Train shall, where applicable:

- clearly identify Risk Train as the sender;
- contain reasonably clear contact details;
- provide a free and reasonable opportunity to opt out of future marketing communications; and
- comply with Applicable Legislation.

## **11.7**

A data subject may opt out of receiving direct marketing communications at any time by:

- following the unsubscribe instructions contained in the communication;
- contacting Risk Train directly; or
- submitting a written request to the Information Officer.

Opting out of marketing communications shall not prevent Risk Train from sending:

- operational communications;
- legal notices;
- certification notifications;
- learner administration communications;
- contractual notices; or
- other non-marketing communications necessary for the provision of services or compliance with legal obligations.

## **11.8**

Risk Train reserves the right to utilise reputable third-party service providers for:

- website hosting;
- email distribution;
- learner management systems;
- online conferencing;
- payment processing;
- analytics;
- cloud storage; and
- operational support services,

provided that such service providers are subject to appropriate confidentiality, security and data protection obligations where required by law.

# **12. UPDATING AND AMENDMENT OF THIS PRIVACY POLICY**

## 12.1

Risk Train (Pty) Ltd (“Risk Train”) reserves the right, at its sole and reasonable discretion, to update, amend, revise, replace or modify this Privacy Policy (“Policy”) from time to time in order to:

- comply with changes in applicable legislation, regulations, codes of conduct or regulatory requirements;
- reflect operational, technological or business changes;
- address evolving cyber-security, privacy or data protection risks;
- improve transparency and data protection practices; or
- ensure ongoing compliance with the Protection of Personal Information Act 4 of 2013 (“POPIA”), the Promotion of Access to Information Act 2 of 2000 (“PAIA”) and other Applicable Legislation.

## 12.2

Any updated or amended version of this Policy shall become effective upon:

- publication on the Risk Train Website;
- circulation through appropriate electronic communication channels;
- implementation within Risk Train’s systems or operations; or
- such later effective date as may be specified in the updated Policy.

## 12.3

Risk Train will take reasonable steps, where appropriate and reasonably practicable, to notify users, learners, clients or other affected data subjects of material amendments to this Policy, including through:

- publication on the Website;
- email communications;
- learner management systems (“LMS”);
- notices on digital platforms; or
- other reasonable communication methods.

## 12.4

Users are encouraged to review this Policy periodically to remain informed regarding how Risk Train processes and protects Personal Information.

## 12.5

Continued access to or use of the Website, systems, services, training platforms or engagement with Risk Train after any amendment to this Policy shall constitute acknowledgement of the updated Policy and acceptance thereof to the extent permitted by law.

## 12.6

No amendment or modification to this Policy shall:

- retrospectively reduce or remove any rights afforded to data subjects under Applicable Legislation;
- permit unlawful processing of Personal Information; or

- limit any statutory obligations imposed on Risk Train under POPIA, PAIA or other Applicable Legislation.

## 12.7

Unless expressly stated otherwise, the latest version of this Policy published by Risk Train shall supersede and replace all previous versions from the effective date of publication.

# 13. CONTACT INFORMATION, COMPLAINTS AND DATA SUBJECT REQUESTS

## 13.1

Questions, concerns, requests or complaints relating to:

- this Privacy Policy;
- the processing of Personal Information by Risk Train (Pty) Ltd (“Risk Train”);
- access to records;
- correction or deletion of Personal Information;
- objections to processing activities;
- withdrawal of consent;
- direct marketing communications;
- security incidents or suspected data breaches; or
- any rights exercised in terms of the Protection of Personal Information Act 4 of 2013 (“POPIA”) or the Promotion of Access to Information Act 2 of 2000 (“PAIA”),

may be directed to Risk Train’s Information Officer using the contact details set out below or elsewhere in this Policy.

## 13.2

### **Information Officer**

Risk Train (Pty) Ltd

### **Email:**

[john@risktrain.co.za](mailto:john@risktrain.co.za)

### **Telephone:**

+27 83 460 1851

### **Website:**

[www.risktrain.co.za](http://www.risktrain.co.za)

### **Physical Address:**

Corner Johan Le Roux and Morris Road  
Meyerton  
Gauteng  
South Africa

Initial

**Postal Address:**

Unit 28  
Pilkington Business Park  
Meyerton  
1961  
South Africa

**13.3**

Risk Train shall take reasonable steps to:

- investigate and respond to complaints or requests;
- verify the identity of persons submitting requests where necessary;
- process requests in accordance with POPIA, PAIA and Applicable Legislation; and
- respond within reasonable or legally prescribed time periods.

**13.4**

Where a data subject is dissatisfied with the manner in which Risk Train has processed Personal Information or handled a complaint, the data subject may lodge a complaint with the Information Regulator of South Africa.

**13.5****Information Regulator South Africa****Website:**

<https://inforegulator.org.za>

**Email:**

complaints.IR@justice.gov.za

**General Enquiries:**

enquiries@inforegulator.org.za

**Physical Address:**

JD House  
27 Stiemens Street  
Braamfontein  
Johannesburg  
South Africa

**13.6**

Nothing contained in this Policy shall limit any rights or remedies available to data subjects under Applicable Legislation.