Equiworks Labour Solutions™

PRIVACY, DATA PROTECTION, WEBSITE USE AND ARTIFICIAL INTELLIGENCE (AI) POLICY

1. INTRODUCTION:

1.1. Equiworks Labour Solutions (Pty) Ltd, registration number: 2024/203236/07 ("Equiworks") recognises the importance of protecting Personal Information and maintaining the confidentiality of information entrusted to it in the course of providing professional labour advisory and workplace governance services. In the ordinary course of its operations, Equiworks collects, processes, stores, and transmits Personal Information relating to clients, employees, service providers, and other stakeholders. This Policy sets out the framework governing how such information is handled in a lawful, transparent, and secure manner.

1.2. Equiworks is committed to complying with the requirements of the Protection of Personal Information Act, Act 4 of 2013 ("POPIA"), which requires responsible parties to process Personal Information in accordance with the conditions for lawful processing, including accountability, purpose limitation, information quality, openness, and security safeguards. This Policy also takes into account the principles of the Promotion of Access to Information Act, Act 2 of 2000 ("PAIA"), where applicable, particularly in relation to access to information and transparency.

1.3. Given the nature of Equiworks' services, which include workplace investigations, disciplinary processes, restructuring advisory, and policy drafting, the organisation routinely handles confidential and, at times, sensitive Personal Information. It is therefore essential that appropriate safeguards are implemented to prevent unauthorised access, disclosure, loss, or misuse of such information. This Policy establishes the minimum standards and controls required to protect Personal Information, whether held in electronic format, hard copy records, or processed through digital platforms.

1.4. This Policy further addresses the responsible use of emerging technologies, including Artificial Intelligence (AI) tools, which may be used to support drafting, research, and operational efficiency. While such tools may enhance service delivery, Equiworks remains committed to ensuring that confidentiality, professional privilege, and data protection obligations are maintained at all times.

1.5. All employees, consultants, contractors, and third parties processing Personal Information on behalf of Equiworks are required to comply with this Policy. Failure to adhere to the provisions of this Policy may result in disciplinary action and, where applicable, legal consequences.

2. PURPOSE:

2.1. The purpose of this Policy is to regulate the lawful collection, processing, storage, protection, and disclosure of Personal Information by Equiworks and to establish standards for data security, website usage, and the responsible use of Artificial Intelligence (AI).

2.2. This Policy is aligned with the:

2.2.1. Protection of Personal Information Act, Act 4 of 2013 ("POPIA")

2.2.2. Promotion of Access to Information Act, Act 2 of 2000 ("PAIA")

2.2.3. Electronic communications and confidentiality principles applicable to professional advisory services

3. SCOPE:

3.1. This Policy applies to all individuals and entities who, in the course of their relationship with Equiworks, collect, access, process, store, transmit, or otherwise handle Personal Information.

3.2. This includes, but is not limited to, employees, consultants, independent contractors, clients, service providers, website users, and any third parties who process information on behalf of Equiworks. All such persons are required to comply with the provisions of this Policy when dealing with Personal Information or confidential information belonging to Equiworks, its clients, or other stakeholders.

3.3. The Policy applies to Personal Information processed in any form, whether electronic or physical. This includes information stored in electronic records, hard copy files, cloud-based storage platforms, shared drives, email systems, mobile devices, and any other digital or physical medium utilised by Equiworks in the course of its operations.

3.4. The Policy further applies to information processed through automated tools or emerging technologies, including Artificial Intelligence (AI) systems, where such tools are used to support drafting, research, data analysis, or other operational functions.

3.5. This Policy therefore governs all stages of the information lifecycle, including the collection, recording, organisation, storage, retrieval, use, dissemination, transmission, retention, and destruction of Personal Information, irrespective of the format in which such information is held or the technology used to process it.

4. DEFINITIONS:

For purposes of this Policy, the following terms shall bear the meanings assigned to them below, unless the context indicates otherwise:

4.1. **"Personal Information"** shall have the meaning ascribed to it in section 1 of the POPIA, and refers to any information relating to an identifiable, living natural person, and where applicable, an identifiable, existing juristic person. This includes, but is not limited to, names, identification numbers, contact details, employment information, disciplinary records, financial information, correspondence, opinions, views, and any other information that may identify a person directly or indirectly. Personal Information also includes information relating to the personal views, professional assessments, and advisory records generated in the course of Equiworks' services.

4.2. **"Special Personal Information"** shall have the meaning assigned in section 26 of POPIA and includes Personal Information relating to a data subject's race, ethnic origin, political persuasion, religious or philosophical beliefs, trade union membership, health or sex life, biometric information, and criminal behaviour to the extent that such information relates to alleged offences or proceedings. The processing of Special Personal Information is subject to stricter controls and may only occur where permitted by POPIA, including where processing is necessary for employment obligations, legal proceedings, or where consent has been obtained.

4.3. **"Processing"** shall have the meaning set out in section 1 of POPIA and includes any operation or activity, whether automated or not, concerning Personal Information. This includes the collection, receipt, recording, organisation, collation, storage, updating, modification, retrieval, consultation, use, dissemination, transmission, distribution, merging, linking, restriction, degradation, erasure, or destruction of Personal Information. Processing also includes the use of Personal Information through digital platforms, cloud services, or Artificial Intelligence tools.

4.4. **"Data Subject"** refers to the natural or juristic person to whom Personal Information relates. This may include employees, clients, contractors, job applicants, service providers, or any other identifiable individual or entity whose Personal Information is processed by Equiworks.

4.5. **"Data Breach"** means any actual or suspected unauthorised access to, acquisition of, disclosure of, loss of, damage to, or compromise of Personal Information. A Data Breach may occur through accidental disclosure, human error, cyber incident, theft of devices, loss of records, unauthorised system access, or any event that compromises the

confidentiality, integrity, or availability of Personal Information. A Data Breach includes circumstances requiring notification in terms of section 22 of POPIA.

5. INFORMATION COLLECTED:

5.1. Equiworks may, in the course of providing professional services, collect and process Personal Information necessary for operational, administrative, and advisory purposes. Such information may include client identification details, including names, contact information, business details, and other information required to establish and maintain professional relationships.

5.2. Equiworks may further collect employment-related information where required for workplace advisory services. This may include employment records, job descriptions, disciplinary information, performance-related documentation, incapacity records, and other HR-related information relevant to the provision of labour and workplace governance services.

5.3. In addition, Equiworks may collect investigation documentation and related materials, including witness statements, reports, findings, and supporting evidence, where such information is necessary for conducting workplace investigations or providing advisory support. Payroll-related information and other remuneration data may also be processed where required for compliance advisory, restructuring support, or employment-related guidance.

5.4. Equiworks may also process general HR records, correspondence exchanged with clients or stakeholders, and contractual documentation necessary for the delivery of services. Website usage data, including information submitted through contact forms or similar communication channels, may be collected for communication, service delivery, and administrative purposes.

5.5. Personal Information shall be collected only where it is necessary for legitimate business purposes, including the provision of professional services, compliance with legal obligations, and the proper administration of Equiworks' operations. All information collected shall be limited to what is reasonably required for the purpose for which it is processed and shall be handled in accordance with the requirements of the POPIA.

6. LAWFUL BASIS FOR PROCESSING:

6.1. Equiworks processes Personal Information in accordance with the lawful grounds set out in section 11 of POPIA. Personal Information may therefore be processed where the data subject has provided consent to such processing, where processing is necessary

for the performance of a contract to which the data subject is a party, where processing is required to comply with a legal obligation imposed on Equiworks, or where processing is necessary for pursuing the legitimate interests of Equiworks or of a third party to whom the information is supplied, provided that such interests are not overridden by the fundamental rights of the data subject.

6.2. Equiworks shall ensure that all processing activities are limited to what is reasonably necessary for the purpose for which the Personal Information is processed and that such processing is conducted in a lawful and transparent manner.

7. DATA SUBJECT RIGHTS:

7.1. In accordance with sections 23 to 25 of the Protection of Personal Information Act, Act 4 of 2013, data subjects have the right to request access to their Personal Information held by Equiworks, to request correction of inaccurate or incomplete information, to request deletion or destruction of Personal Information where appropriate, to object to the processing of their Personal Information on reasonable grounds, and to withdraw consent where processing is based on consent.

7.2. Equiworks shall consider such requests in accordance with the applicable legislative requirements.

7.3. Personal Information shall be destroyed, deleted, or de-identified where it is no longer required for the purpose for which it was collected, where the data subject withdraws consent and there is no other lawful basis for processing, where processing is unlawful, or where deletion is required to comply with a legal obligation.

7.4. All destruction or deletion of Personal Information shall be conducted in a secure manner consistent with Equiworks' data retention and disposal procedures.

8. DATA STORAGE:

8.1. Equiworks stores Personal Information in a variety of formats and systems necessary for the efficient delivery of its services and the administration of its operations. Personal Information may be stored on company servers, approved cloud-based systems, company-issued devices, secure physical files, and backup systems maintained for business continuity and data recovery purposes. Such storage may include both electronic and hard copy records, depending on operational requirements.

8.2. All Personal Information shall be stored in a manner that ensures appropriate security safeguards and protects against unauthorised access, loss, damage, or disclosure. Access to stored information shall be restricted to authorised personnel who require

such access for legitimate business purposes, and reasonable technical and organisational measures shall be implemented to safeguard the integrity and confidentiality of the information. These measures may include password protection, access controls, encryption where appropriate, secure physical storage, and controlled backup procedures.

8.3. The storage of Personal Information shall at all times comply with the requirements of section 19 of the Protection of Personal Information Act, Act 4 of 2013, which obliges responsible parties to secure the integrity and confidentiality of Personal Information by taking appropriate, reasonable technical and organisational measures to prevent loss, damage, unauthorised destruction, or unlawful access.

9. DATA SECURITY MEASURES:

9.1. Equiworks implements appropriate and reasonable technical and organisational measures to safeguard the integrity and confidentiality of Personal Information in its possession or under its control, in accordance with section 19 of the Protection of POPIA. These measures are designed to prevent loss, damage, unauthorised access, disclosure, or unlawful processing of Personal Information.

9.2. Such measures include, but are not limited to, the implementation of access control systems to ensure that Personal Information is accessible only to authorised personnel on a need-to-know basis, the use of secure password protection protocols, and the application of encryption where appropriate, particularly in relation to the transmission or storage of sensitive information. Personal Information is stored in secure environments, whether electronically or in hard copy, with restricted access and appropriate physical and digital safeguards.

9.3. Equiworks further ensures that all devices used to access or process Personal Information are secured, including through device locking mechanisms and controlled user access. Anti-virus and anti-malware protections are implemented and maintained to protect against external threats, and regular backups are conducted to ensure data integrity and business continuity. Where appropriate, documents containing Personal Information are clearly marked as confidential to reinforce handling requirements.

9.4. All personnel are required to handle Personal Information with due care and in accordance with this Policy. Personal Information may not be shared informally or disclosed without proper authorisation, must not be left unattended or exposed to unauthorised persons, and must not be transmitted through unsecured or inappropriate channels. Any deviation from these requirements may compromise the security of Personal Information and may result in disciplinary action.

10. ACCESS CONTROL:

10.1. Access to Personal Information held by Equiworks shall be strictly controlled and limited to authorised personnel who require such access for legitimate business and operational purposes.

10.2. Access shall be granted on a role-based basis, ensuring that individuals are provided only with the level of access necessary to perform their duties.

10.3. Appropriate access controls shall be implemented to prevent unauthorised viewing, modification, or disclosure of Personal Information, and where reasonably practicable, access to systems containing Personal Information shall be logged and monitored to maintain accountability and traceability.

10.4. All systems used to store or process Personal Information shall be protected by secure authentication mechanisms, including password protection or other approved security controls.

10.5. Passwords must be treated as confidential at all times and must not be shared with any other person. Users are responsible for safeguarding their login credentials and must ensure that passwords are sufficiently strong and not easily guessable. Where there is any reason to believe that a password has been compromised, it must be changed immediately and the matter reported to the appropriate responsible person.

11. ARTIFICIAL INTELLIGENCE (AI) USE:

11.1. Equiworks recognises that Artificial Intelligence ("AI") tools may be utilised to support the efficient delivery of professional services, including the preparation of documentation, research assistance, and the improvement of administrative processes. The use of AI is intended to enhance productivity and support decision-making, while ensuring that professional judgement and confidentiality obligations remain paramount.

11.2. AI tools may be used for purposes such as drafting and refining documents, conducting preliminary research, editing and improving language, structuring policies and agreements, and developing templates. The use of such tools is limited to supporting functions and does not replace professional review, legal analysis, or the application of expert judgement.

11.3. Where AI tools are utilised, limited Personal Information may be included where necessary to provide sufficient context for accurate outputs. In such instances, only information that is relevant to the specific task should be used, and, where reasonably practicable, sensitive or highly confidential information should be avoided. Personnel must exercise professional discretion at all times and ensure that the use of AI tools does

not compromise confidentiality, professional privilege, or the obligations imposed by the Protection of Personal Information Act, Act 4 of 2013.

11.4. All outputs generated through AI tools must be subject to appropriate human oversight. AI-generated content must be reviewed, verified for accuracy, and approved by an authorised Equiworks representative prior to being relied upon or shared externally. Equiworks retains full responsibility for all documents and advice produced with the assistance of AI tools, and the use of AI does not transfer or diminish professional accountability.

12. CONFIDENTIALITY:

12.1. All personnel of Equiworks, including employees, consultants, contractors, and any third parties acting on behalf of Equiworks, are required to maintain the confidentiality of all Personal Information and confidential information accessed or processed in the course of their duties. Such confidentiality obligations arise from applicable legislation, including the POPIA, as well as professional standards governing advisory services and any contractual confidentiality undertakings entered into with clients, service providers, or other stakeholders.

12.2. Confidential information includes, but is not limited to, client information, employee records, investigation documentation, advisory reports, commercial information, and any other information not intended for public disclosure. Personnel must ensure that such information is handled with appropriate care and is accessed, used, and stored only for legitimate business purposes.

12.3. Confidential information may not be disclosed, shared, or communicated to any unauthorised person without proper authorisation, unless disclosure is required by law or is necessary for the performance of authorised duties. Any unauthorised disclosure or misuse of confidential information may constitute a breach of this Policy and may result in disciplinary action and, where applicable, legal consequences.

13. RETENTION OF PERSONAL INFORMATION:

13.1. Equiworks shall retain Personal Information only for as long as is necessary to fulfil the purpose for which such information was collected or subsequently processed, in accordance with section 14 of the POPIA. Personal Information shall not be retained for longer than is reasonably required, unless retention is necessary for lawful purposes, including compliance with legal obligations, the establishment, exercise, or defence of legal rights, or for legitimate operational requirements.

13.2. Retention periods shall be reviewed periodically to ensure that Personal Information is not held longer than necessary. Where Personal Information is no longer required for the purpose for which it was collected, and there is no lawful basis for continued retention, such information shall be securely destroyed, deleted, or de-identified in accordance with Equiworks' data disposal procedures.

13.3. Notwithstanding the above, Equiworks may retain Personal Information for longer periods where such retention is required for legal, regulatory, or contractual purposes, including but not limited to compliance with statutory record-keeping obligations or for the purpose of managing or defending legal claims.

14. DISPOSAL OF PERSONAL INFORMATION:

14.1. Upon expiry of the applicable retention period, or where Personal Information is no longer required for the purpose for which it was collected, Equiworks shall ensure that such information is disposed of in a secure manner to prevent unauthorised access, disclosure, or reconstruction. The disposal of Personal Information shall be conducted in accordance with section 14 of the POPIA and in line with appropriate security safeguards.

14.2. Electronic records containing Personal Information shall be permanently and securely deleted using methods designed to prevent recovery or reconstruction of the data. Hard copy records shall be destroyed through secure means, including shredding or other appropriate destruction processes. Where Special Personal Information is involved, additional care shall be taken to ensure that such information is irreversibly destroyed in a manner that safeguards confidentiality.

14.3. Equiworks shall ensure that disposal procedures are implemented consistently and that only authorised personnel are permitted to undertake the destruction of Personal Information. Any third parties engaged to assist with the disposal process must be subject to confidentiality obligations and appropriate data protection safeguards.

15. DATA BREACH MANAGEMENT:

15.1. Equiworks shall manage any compromise of Personal Information in accordance with section 22 of the POPIA. A data breach includes any actual or suspected unauthorised access to, acquisition of, disclosure of, loss of, or compromise of Personal Information. Such incidents may arise from, inter alia, the loss or misplacement of records, theft of devices containing Personal Information, unauthorised disclosure to third parties, cyber security incidents, system vulnerabilities, or human error.

15.2. Where a data breach is identified or reasonably suspected, Equiworks shall take immediate steps to investigate the incident and assess its scope and potential impact. The investigation shall include determining the nature of the Personal Information affected, the extent of the breach, the potential risks to data subjects, and the steps required to contain the breach and prevent further compromise. Appropriate measures shall be implemented without delay to contain the breach and mitigate any adverse consequences.

15.3. Where required by section 22 of POPIA, Equiworks shall notify affected data subjects as soon as reasonably possible, providing sufficient information to enable them to take protective measures where necessary. In addition, the Information Regulator shall be notified where the breach involves a compromise of Personal Information and notification is required by law. All data breaches shall be documented, and corrective measures shall be implemented to reduce the likelihood of recurrence.

16. INTELLECTUAL PROPERTY:

16.1. All content made available on Equiworks website, including but not limited to text, policies, templates, training materials, graphics, logos, branding, and any other proprietary material, remains the intellectual property of Equiworks or its licensors. Such content is protected by applicable intellectual property laws and may not be used in a manner that infringes these rights.

16.2. Users of the website or recipients of Equiworks materials may not copy, reproduce, distribute, publish, adapt, or otherwise make use of any content, in whole or in part, without the prior written consent of Equiworks. Limited use of such content for personal, non-commercial, or informational purposes is permitted, provided that the content is not altered and appropriate acknowledgement of Equiworks' ownership is maintained.

16.3. Any unauthorised use, reproduction, or distribution of Equiworks' intellectual property may constitute an infringement of intellectual property rights and may result in appropriate legal action.

17. SOFTWARE USE AND ANTI-VIRUS SECURITY:

17.1. Equiworks utilises various software applications and digital platforms in the delivery of its services. The use of such software must be managed in a manner that safeguards Personal Information and protects the integrity of the organisation's systems and data. All software usage must therefore comply with the security safeguard obligations contained in section 19 of the Protection of Personal Information Act, Act 4 of 2013,

which requires appropriate technical and organisational measures to prevent loss, damage, or unauthorised access to Personal Information.

17.2. All software used by Equiworks must be legitimate, properly licensed, and approved by management prior to installation. No employee, consultant, or contractor may install software on company devices or systems without authorisation. This includes applications downloaded from the internet, browser extensions, file-sharing tools, or remote access software. The installation of unauthorised software may expose the organisation to malware, data leakage, or system vulnerabilities and is therefore prohibited.

17.3. All software, including operating systems, applications, and security tools, must be kept up to date. Security patches, updates, and fixes must be installed as soon as reasonably practicable to address known vulnerabilities. Where a software application is identified as presenting a security risk, Equiworks reserves the right to restrict, suspend, or remove such software from company systems.

17.4. Equiworks shall ensure that appropriate anti-virus, anti-malware, and firewall protection is installed on all company devices, including laptops and desktops used to process Personal Information. Anti-virus software must be configured to:

17.4.1. automatically update virus definitions;

17.4.2. perform regular system scans;

17.4.3. monitor files in real time; and

17.4.4. detect and quarantine suspicious files.

17.5. All devices used to process company information must be protected by active anti-virus software. No anti-virus software may be disabled or removed without authorisation. Where a virus, malware, or suspicious activity is detected, the user must immediately report the incident to the responsible manager or Information Officer, and the device must not be used until it has been assessed and cleared.

17.6. External storage devices, including USB drives, external hard drives, or memory cards, must be scanned for viruses before files are opened or transferred. Similarly, files received via email or downloaded from the internet must be treated with caution and, where appropriate, scanned prior to use.

17.7. Where Personal Information is shared electronically, reasonable steps must be taken to ensure that the files are secure and free from malicious code. Any suspected cyber security incident, including phishing emails, suspicious attachments, or unauthorised system access, must be reported immediately.

17.8. Failure to comply with software security and anti-virus requirements may result in disciplinary action, as such conduct may expose Equiworks and its clients to significant confidentiality and data protection risks.

18. GOVERNING LAW:

18.1. This Policy shall be governed by and interpreted in accordance with the laws of the Republic of South Africa. In particular, this Policy is aligned with and subject to the provisions of the Protection of Personal Information Act, Act 4 of 2013, and the Promotion of Access to Information Act, Act 2 of 2000, together with any regulations issued thereunder.

18.2. To the extent that any provision of this Policy is inconsistent with applicable legislation, the relevant statutory provisions shall prevail, and this Policy shall be interpreted accordingly.

19. POLICY IMPLEMENTATION DETAILS:

Item	Details
Policy Name	Privacy, Data Protection, Data Security and AI Policy
Organisation	Equiworks Labour Solutions (Pty) Ltd
Effective Date	01 April 2026
Approved By	Lerato Ncube
Responsible Person	Managing Director
Next Review Date	01 April 2027
Review Frequency	Annually or as required