Data Privacy and Information Security Policy

Version 1.2 **August 2021**

Data Privacy and Information Security Policy

1. Introduction

Data privacy is the rights and obligations of individuals and organisations with respect to the collection, use, retention and disclosure of personal information.

Information security is the protecting measures implemented by an organisation to protect the integrity of such data and information within that organisation from a wide range of threats in order to adhere to applicable legislation and to ensure business continuity, minimise business risk and optimise returns on investment.

2. Preamble

Data privacy and Information security is an integral component of the Risk Management structure of EMPOWERisk Management Services (Pty) Ltd, hereinafter referred to as the "Company".

The Company has an obligation to ensure appropriate security for all Information Technology (IT) systems (data, equipment and processes) and personal information that it owns and/or controls on behalf of other responsible parties.

Appropriate levels of security will be determined by a risk assessment, i.e., assessment of threats to, impacts on and vulnerabilities of IT systems and information and the likelihood of their occurrence.

The need for data privacy and information security is driven by the following:

a. Legal, statutory, regulatory and contractual obligations;
b. Risk assessment;
c. Operational principles, objectives and requirements for information systems that the Company has defined or developed.

3. Policy application

This policy will apply to:

a. The Company;
b. Any joint ventures, and/or other business organisations that are owned or controlled by the Company who receive or process personal information for, or on behalf of the Company;
c. The employees and independent contractors of the Company; and
d. Personal information of external data subjects and data owners processed and/or stored by the Company, as well as the personal information of Company personnel.

4. Policy scope

The policy will be promulgated to include the following domains and frameworks:

4.1 Logical security

a. **Data security** - Inclusive of data privacy principles, confidentiality, criticality, integrity and intellectual property rights;
b. **Communications security** - Establishing network connections, flow control systems inclusive of firewalls, encryption, dial-up communications, telephone systems, electronic mail systems, downloaded data, internet connections and telecommuting arrangements;
c. **Software security** - Inclusive of system access control and password management; privilege control and logging; and
d. **Software development and change control** - Inclusive of change control processes for workstations; third party involvement; handling of viruses and worms and software development processes.

4.2 Physical security

a. **Physical access security** - Inclusive of building and computer facilities access control; and
b. **Computer location and environment** - Inclusive of premises, emergency data centre premises and their construction, emergency power supply and equipment; alarm systems and contingency planning for emergency situations.

4.3 Managerial security

a. **Administrative security** - Inclusive of user training and awareness; reporting of security problems and information security breach incidents; controls and risk assessment; outsourcing and third-party contracts;
b. **Human Resource** - Inclusive of a separate, but consequential human resources policy with alignment to relevant data privacy and information security principles and regulations, background checks, application and appointment procedures, qualifications and skills, disciplinary code and protection of personal information agreements; and
c. **Business Continuity Management** - Inclusive of a separate, but consequential business continuation and disaster recovery plan with contingency planning, testing of plans, identification and minimisation of business and information security risks.

5. Terms and definitions

a. **Asset** – anything that has value to the organisation.
b. **Biometrics** – means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.
c. **Consent** – means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
d. **Control** – means of managing risk, including policies, procedures, guidelines, practices or organisational structures, which can be of administrative, technical, management, or legal nature (**Please note**: Control is also used as a synonym for safeguard or counter measure).
e. **Data controller** – a mandated individual who decides on the manner and purpose for which personal information is processed.

f. **Data owner** –for the purposes of this document, means the owner of personal information or data obtained by implicit or explicit consent of an individual (i.e. banking institutions).

g. **Data privacy** – for the purposes of this document, data privacy is the act of securing personal data within an organisation by following good practice security procedures and implementing controls in order to confirm that personal data is secure.

h. **Data subject** – the person or persons about whom personal information is collected, stored or processed.

i. **Disclosure** – in general terms personal information is disclosed when it is released to parties outside the organisation. It does not include giving individuals information about themselves.

j. **Guideline** – a description that clarifies what should be done and how, to achieve the objectives set out in policies.

k. **IMC** – for purposes of this document, refers to the Information Management Committee of a private body.

l. **Information Management Committee** – for the purposes of this document, means a decision-making structure in a private body to control, regulate and enforce Information Security policy requirements.

m. **Information officer** – means the head or duly authorised person of a private body as contemplated in Section 1 of the Promotion of Access to Information Act of 2000.

n. **Information processing facilities** – any information processing system, service or infrastructure, or the physical locations housing them.

o. **Information security** – preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, nonrepudiation, and reliability can also be involved.

p. **Information security event** – means an identified occurrence of a system, service or network that is indicating a possible breach of information security policy prescription, or failure of safeguards, or a previously unknown situation that may be security relevant.

q. **Information security incident** – an information security incident is indicated by a single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

r. **Legal entity** – for the purposes of this document, the term legal entity is applied to any organisation within the same ownership chain as an organisation who processes a data owners' personal information and may include joint ventures (consolidated or unconsolidated), parent companies or any other organisation contracted by the data owner. All direct legal entities are required to adhere to the data owners' requirements for data privacy and information security.

s. **Media** – any means of containment of data and information by way of, i.e. written documentation, compact disc (CD), digital video disc or digital versatile disc (DVD), audio, visual recording, computerised filing, etc. – in context also referring to public news reporting entities, i.e. newspapers, radio and television reporters or representatives.

t. **Personal information** – for the purposes of this document and in line with pending South African legislation, personal information means information relating to an identifiable, living, natural person and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

- information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or

mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- the biometric information of the person;
- the personal opinions, views, expressions or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the person; and
- the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person

All of the above is inclusive of information related to next of kin and information that is recorded in electronic formats (e.g. in databases, Word documents, Excel spreadsheets, email, closed circuit television (CCTV), voice recordings etc.) and all information about the person recorded in structured hard copy filing systems (e.g. personnel files).]

u. **Policy** – overall intention and direction as formally expressed by management.

v. **Processing/Data processing** – any operation or set of operations which is performed upon personal information, whether or not by automatic means, such as collection, recording, organising, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

w. **Production data** – data that is used and/or produced during the normal day-to-day operations in the organisation.

x. **Regulator** –means the Information Regulator established in terms of Section39 of the Protection of Personal Information Act.

y. **Responsible party** – means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

z. **Risk** – combination of the probability of an event and its consequence.

aa. **Risk analysis** – systematic use of information to identify sources and to estimate the risk.

bb. **Risk assessment** – overall process of risk analysis and risk evaluation.

cc. **Risk evaluation** – process of comparing the estimated risk against given risk criteria to determine the significance of the risk.

dd. **Risk management** – coordinated activities to direct and control an organisation with regard to risk. Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication.

ee. **Risk treatment** – process of selection and implementation of measures to modify and reduce risk.

ff. **Sanitation** – for the purposes of this document, sanitation is the process of removing all traces of a data subject- or owner's personal information from hard drives and other data storage media, before such equipment is exchanged, sold, discarded, passed to a new user or used for non-company purposes.

gg. **Test data** – data that is specifically recorded for test purposes and is not used for day-today operations within the organisation.

hh. **Third party/subcontractor** – any entity, whether an individual or a company, who is not part of a responsible party's organisational structure, but works with the responsible party, or processes personal information on the responsible party's behalf.

ii. **Threat** – a potential cause of an unwanted incident, which may result in harm to a system or organisation.

jj. **Vulnerability** – a weakness of an asset or group of assets that can be exploited by one or more threats.

6. Management intent

Against the background of the aforementioned, it is therefore the focused intent of the Company to incorporate all the applicable principles and regulations in this policy and to monitor and enforce compliance to its prescriptions by way of establishing the necessary mandated management and reporting structures to facilitate these outcomes.

6.1 Objectives

In order to create effective and visible guidelines for the Company, its employees and any associated third-party alliances or subcontractors, this policy has been specifically designed to meet the necessary compliance standards regarding the following aspects:

a. Management of information security and data privacy within the structure of the Company;
b. To manage and maintain the security of information and data processing facilities that are accessed, processed, communicated to, or managed by external parties;
c. To ensure that all data and personal information receives an appropriate level of protection;
d. To ensure that employees, contractors and third-party users of the Company understand their responsibilities and are suitable for the roles they perform, or are considered for and to reduce the risk of theft, fraud or misuse of facilities;
e. To ensure that employees, contractors and third-party users of the Company are aware of personal information and data security, security threats and concerns, their responsibilities and liabilities and are equipped to support the organisational information technology policy of the Company in the course of their normal work and to reduce the risk of human error;
f. To ensure that employees, contractors and third-party users of the Company exit the employment or change employment in an orderly manner;
g. To prevent unauthorised physical access and damage to, or interference with the premises, data or personal information related to the Company;
h. To ensure the correct and secure operation of all data and information processing facilities within the Company;
i. To implement and maintain the appropriate level of data and information security and service delivery agreements;
j. To minimise the risk of system failures;
k. To protect the integrity of software data and personal information;

l. To maintain the integrity and availability of back-up of data, information and related processing facilities;
m. To ensure the protection of data and personal information in any networks related to the Company, as well as protection of the supporting infrastructure;
n. To prevent unauthorised disclosure, modification, removal or destruction of removable assets and media under the control of the Company;
o. To ensure the security of electronic commerce services (where applicable) and their secure use within the Company;
p. To detect unauthorised data and information processing activities within the Company;
q. To ensure proper, authorised user access and to prevent unauthorised access and the compromise or theft of data and information of the Company;
r. To prevent unauthorised user access and the compromise or theft of personal information or data from data / information processing facilities related to the operations and functions of the Company;
s. To prevent unauthorised access to networked services if and when applicable;
t. To prevent unauthorised access to the Company operating systems;
u. To prevent unauthorised access to data and personal information held in any application systems within the Company;
v. To ensure data and information security if and when mobile computing and teleworking facilities are employed by the Company;
w. To ensure that security is an integral part of all relevant data and information systems in use by the Company;
x. To prevent errors, loss, unauthorised modification or misuse of data and personal information in applications within the Company;
y. To protect the confidentiality, authenticity or integrity of data and personal information within the Company by cryptographic means;
z. To ensure the security of system files;
aa. To maintain the security of application software, data and information within the Company;
bb. To reduce risks resulting from exploitation of published technical vulnerabilities;
cc. To ensure that any breach in information and data security events and weaknesses associated with information systems within the Company are communicated in a manner allowing timely corrective action to be taken;
dd. To counteract interruptions to business activities and to protect critical business processes within the Company from the effects of major failures of data and information systems or disasters and to ensure their timely resumption;
ee. To avoid violations of any law, statutory, regulatory or contractual obligations and of any security requirements;
ff. To ensure compliance of systems used by the Company within its organisational security policies and standards and
gg. To maximise the effectiveness of, and to minimise interference to or from the information and data systems audit process.

7. Management subscription

The management of the Company subscribes to the goals and principles of data and information security in line with relevant legislation and its business strategy and objectives.

The relationship of the Company with its personnel, clients and associates is based on mutual integrity and trust and it is therefore committed to maintaining this trust by protecting the privacy of personal information and data disclosed and received from any data subject or data owner at all times and to the best of its ability.

As part of this commitment, the Company will subscribe in all material respects to the following:

a. Protection Of Personal Information Act 2013;
b. Promotion of Access to Information Act 2000;
c. Applicable guidelines as per the SA National Standard (ISO/SANS 27002:2008); and
d. Generally Accepted Privacy Principles (G.A.P.P), consisting of the following:

i) **Management** - the Company defines documents, communicates and assigns accountability for its privacy policies and procedures;
ii) **Notice** - the Company provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed;
iii) **Choice and consent** - the Company describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use and disclosure of personal information;
iv) **Collection** - the Company collects personal information only for the purposes identified in the notice;
v) **Use and retention** - the Company limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent and retains the information for only as long as necessary to fulfil the stated purposes
vi) **Access** - the Company provides individuals with convenient access to their personal information for review and updates;
vii) **Disclosure (to third parties**) - the Company discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual;
viii) **Security (for privacy)** - the Company protects personal information against unauthorised access (both physical and logical);
ix) **Quality** - the Company maintains accurate, complete and relevant personal information for the purposes identified in the notice; and
x) **Monitoring and enforcement** - the Company monitors compliance with its Information Security policies and procedures and has procedures to address privacy-related complaints and disputes.

8. Management control and enforcement

8.1 Information Officer

In order to comply with legislation and to facilitate and manage the outcomes of

the declared intent of the management of the Company regarding this policy, the Information Officer for the Company will be the Chief Executive Officer or a duly authorised person of the Company according to the requirements as defined under Section 1 of the Protection of Personal Information Act 2013 and read together with the prescriptions of Section 1 of the Promotion of Access to Information Act 2000.

The Information Officer will be duly registered with the Information Regulator as is required by the applicable legislation after its establishment and will report to the Board of Directors of the Company.

The role and responsibilities of the Information Officer and by delegation the duly authorised person, will be included in a formalised and documented job description for assessment and regulatory purposes and also to facilitate compliance to Section 55 of the Protection of Personal Information Act 2013.

The officer and duly authorised person will perform in their respective capacities immediately after appointment, but will officially only take up their duties in terms of this Act after the establishment of the Information Regulator and their subsequent registration with the Regulator.

8.2 Breach of information security event

a. Definition

A breach of information security event can be defined as “the actual or potential loss of personal data and/or any information that could lead to identity fraud or have any other significant impacts on individuals or the Company”.

b. Application

The prescriptions applicable to this matter will apply to all Company personnel and third-party service providers under contract to the Company.

c. Identification of event/incidents

The following are common examples of events, which include but is not limited to:

i. Loss or damage to paper-based files containing classified or personal identifiable information;
ii. Loss of computer equipment due to crime or an individual’s carelessness;
iii. Loss of unencrypted computer media e.g. compact disc (CD), data stick, laptop or other portable device;
iv. Corrupted data;
v. Access to inappropriate websites in breach of policy;
vi. Theft;
vii. Fraud;
viii. A computer virus;
ix. Successful hacking attack;

x. Accessing a system or computer using someone else's authorisation code, either fraudulently or by accident;
xi. Forced entry gained to a secure room/building housing classified information;
xii. Finding classified or confidential Company information outside Company premises;
xiii. Finding Company paper or electronic records about identifiable individuals in any location outside of the Company premises;
xiv. Discussing personnel or any other data subject's personal information with someone else in an open area where the conversation can be overheard by outsiders;
xv. Personal identifiable information sent by insecure means/lost in transit (e.g. payslips, human resources records, financial statements, copies of identity documents, etc.);
xvi. Unauthorised copying of, or removal of personal identifiable information;
xvii. A fax, email or paper document with personal identifiable information sent to the incorrect recipient;
xviii. Evidence of tampering/damage to data cabling between server and work stations or cabling not installed to acceptable industry safety standards;
xix. Unsecured handling of information storage systems/equipment during a period of disaster or serious damage to the housing complex due to e.g. fire, flooding, earthquake, sabotage, etc.;
xx. Evidence of unauthorised cameras, monitoring devices, or listening equipment in the information processing facilities;
xxi. Suspicious unaccompanied persons wandering around in information security areas;
xxii. Allowing uncleared and/or un-identified third party I/T or other contractor personnel to work on information security systems of the Company.
xxiii. Evidence of unattended and unsecured information processing workstations not securely logged-off during the absence of the operator;
xxiv. Evidence of weak or no appropriate password management/log-on procedures; and
xxv. Any violation of related security protocols as prescribed by the Company Information Security Policy that can possibly lead to the loss of classified information.

d. Reporting process

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the Company is obliged under Section 22, subsection 1 of the Protection of Personal Information Act (pending) to notify the Regulator and also (subject to subsection 3) the data subject of the event/incident.

Under this policy all Company employees and third-party contractors to the Company are obligated to report any breach, or suspected breach of information security immediately to the Company via a prescribed process.

The prescribed process for reporting any breach of information security event related to any personal information owned by, or under control of the Company, will be that any person that has any knowledge or evidence of such an occurrence will be obliged to make a written initial report regarding the incident immediately after acquiring the knowledge or evidence of the incident to the Information Officer, or in his/her absence, to any of the members of the Information Management Committee.

A compulsory breach of information security event report must be fully completed by the person witnessing or discovering the incident immediately after the initial report and submitted to the Information Officer, or in his/her absence, to any of the members of the Information Management Committee.

Please note - A signed copy of this report must be retained as receipt by the person that submits the report.

Only the Information Management Committee will be mandated to make a factual assessment of the incident in order to take whatever remedial steps necessary to contain the situation and also for the regulatory reporting of the incident to the Information Regulator, data subject and data owner where it is deemed to be appropriate and applicable.

No other employee or any third-party contractor of the Company will have any mandate to decide on the merits, or applicability of any reports in this category, unless specifically authorised to this effect in writing by the management of the Company.

Any violation of this prescription will be addressed via the disciplinary code, or the third-party management prescriptions of the Company as is applicable.

e. Accountability

Any employee that is found to be responsible for an event where a breach of information security occurs through negligence, or non-compliance to the Company's policy prescriptions, or any person that has knowledge of such an occurrence and fails to report the incident for whatever reason, will be held fully accountable for the incident and subjected to the disciplinary code and procedure of the Company.

The contractual agreements of external third-party contractors to the Company will be subject to immediate suspension or termination in the sole discretion of the management of the Company, pending investigation and recommendations of the Information Management Committee of the Company.

In the event of a monetary loss to the Company as a direct result of the occurrence of the breach in information security, the responsible party, or parties in both instances may be held fully liable for the loss and any costs for recovery thereof in the sole discretion of the management of the Company.

f. Enforcement

The severity of any disciplinary or other enforcement action taken by the Company will vary based on factors considered relevant by the Information Management Committee, including but not limited to:

a. The sensitivity of the personal data disclosed or used in violation of this policy;
b. The number of parties impacted by the violation of this policy;
c. The duration of the improper disclosure or unauthorised use;
d. Prior improper disclosure or use of personal information by any applicable accountable party; and
e. Whether the violation or neglect was inadvertent or the result of inadequate training, or supervision.

Please note: Where the Information Management Committee believes that the conduct may constitute a violation of any applicable law, rule, or regulation, the conduct may be disclosed to appropriate law enforcement and regulatory authorities.

9. Third party management

All third-party agreements with the Company will make provision for the clauses and conditions necessary for these parties to comply with the information security requirements in terms of this Policy and the remedial procedures to enforce these requirements.

The strict compliance of third parties to the conditions contained in the relevant agreements will be monitored by the Information Officer or delegated Deputy Information Officer/(s) of the Company as part of their job description and any violations reported to the Information Management Committee for assessment and remedial actions where appropriate

10. Dealing with public media

Only Management or designated representatives of the Company will be authorised to make any presentation, comment, statement or direct contact with the public media regarding any matter whatsoever regarding any Information Security incident, client information or any business issues directly related to the organisation and/or its operations.

Any employee, contractor, or associated third party that is found in violation of this ruling will be subjected to the applicable sanctions in accordance with the Company's disciplinary code and/or any other related policy governance as may be applicable.

11. Revision of the policy

The policy will be reviewed on an annual basis to address any changes in the technical domain, or applicable legislation.

In the event of any critical interim developments regarding the above, immediate revision and adaption will be implemented as soon as reasonably possible and the revised documentation circulated and explained to all relevant parties through the Company's awareness programs and/or information sessions.

The revision history index of the Policy will then also be updated accordingly.

12. Related legislation, policies, documentation and agreements

a. Protection of Personal Information Act of 2013;
b. Promotion of Access to Information Act of 2000;
c. Companies Act of 2008;
d. King III Code of Governance Principles;
e. Generally Accepted Privacy Principles (GAPP)
f. Company business continuation and disaster recovery plan; and
g. Human resources policy as well as disciplinary code and procedure.