DOCUMENT NAME: INFORMATION BREACH POLICY	
DOCUMENT TYPE: POPI POLICY	

1. INTRODUCTION

- This Policy and Plan aims to help the Company manage personal Information breaches effectively.

- The Company holds Personal Information about our users, employees, clients, suppliers and other individuals for a variety of business purposes.

- The Company is committed to the correct, lawful, and fair handling of all Personal Information, respecting the legal rights, privacy and trust of all individuals with whom it deals.

- An Information breach generally refers to the unauthorised access and retrieval of information that may include corporate and / or personal information. Information breaches are generally recognised as one of the more costly security failures of organisations.

- They could lead to financial losses, and cause consumers to lose trust in the Company or our clients.

- The regulations across the various jurisdictions in which the Company operates require the Company to make reasonable security arrangements to protect the Personal Information that we possess or control, to prevent unauthorised access, collection, use, disclosure, or similar risks.

2. SCOPE

- This policy applies to all staff who must be familiar with this policy and comply with its terms.

- This policy supplements other policies relating to internet and email use.

- The Company may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

- As our Information Officer, **Dr Lezelle Floyd** has overall responsibility for the day-to-day implementation of this policy.

3. TRAINING

- All staff will receive training on this policy.
- New staff will receive training as part of the induction process.
- Further training will be provided at least every year or whenever there is a substantial change in the law or our policy and procedure.
- Training is provided through an in-house workshop, and covers the applicable laws relating to Information protection, and the Company's Information protection and related policies and procedures.
- Completion of training is compulsory.
- Any Questions can be directed to the Information Officer.

4. APPLICABLE LEGISLATIVE CONSIDERATIONS

- Protection of Personal Information Act 4 of 2013 & Regulations thereto.
- According to the Act, Personal Information means information relating to a person and includes all information about that person, including their characteristics and identifying information and correspondence that are implicitly or explicitly of a private or confidential nature. (The definition provided in POPIA is wide and requires careful consideration.)
- The Company defines Personal Information as the broader of the definitions contained in the Act.
- Any use of Personal Information is to be strictly controlled in accordance with this policy.
- While some Information will always relate to an individual (natural or juristic), other Information may not, on its own, relate to an individual. Such Information would not constitute Personal Information unless it is associated with, or made to relate to, a particular data subject.
- Generic information that does not relate to a particular individual may also form part of an individual's Personal Information when combined with Personal Information or other information to enable an individual to be identified.

5. AGGREGATED INFORMATION IS NOT PERSONAL INFORMATION

- The Company gathers Personal Information for two purposes, to identify and protect the Information given to us by our customers, and for internal operations.

- Personal Information we gather for internal operational purposes relates to identifiable individuals such as job applicants, current and former employees, contract and other staff, clients, suppliers, and marketing contacts, and the Information gathered may include individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.

6. CAUSES OF INFORMATION BREACHES

Information breaches may be caused by employees, parties external to the organisation, or computer system errors.

Human Error

Human Error causes include:

- Loss of computing devices (portable or otherwise), Information storage devices, or paper records containing personal Information.
- Disclosing Information to a wrong recipient
- Handling Information in an unauthorised way (for example: downloading a local copy of personal Information)
- Unauthorised access or disclosure of personal Information by employees (for example: sharing a login)
- Improper disposal of personal Information (for example: hard disk, storage media, or paper documents containing personal Information sold or discarded before Information is properly deleted)

Malicious Activities

Malicious causes include:

- Hacking incidents / Illegal access to Information bases containing Personal Information.
- Hacking to access unauthorised Information via the Coaching App or API.

- Theft of computing devices (portable or otherwise), Information storage devices, or paper records containing Personal Information.
- Scams that trick the Company staff into releasing Personal Information of individuals.

Computer System Error

Computer System Error causes include:

- Errors or bugs in the Company's Application, or API
- Failure of cloud services, cloud computing or cloud storage security / authentication / authorisation systems

7. REPORTING BREACHES

All members of staff have an obligation to report actual or potential Information protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary.
- Maintain a register of compliance failures.
- Notify the Information Regulator of any compliance failures that are material either in their own right or as part of a pattern of failures.

Under the Act, the Company is legally obliged to instances where personal information has been compromised, notify the Regulator and the data subject, unless the identity of the data subject cannot be established. (Section 22).

Individuals must be notified if adverse impact is determined.

In addition, the Company must notify any affected clients without undue delay after becoming aware of a personal Information breach.

8. INFORMATION BREACH TEAM

- The Information Breach Team consists of the CEO/Director, Information Officer and Deputy Information Officer
- The CEO/Director has the responsibility to make all time-critical decisions on steps taken to contain and manage the incident.

The notification should include the following information, where available:

- Extent of the Information breach.
- Type and volume of personal Information involved.
- Cause or suspected cause of the breach.
- Whether the breach has been rectified.
- Measures and processes that the organisation had put in place at the time of the breach.
- Information on whether affected individuals of the Information breach were notified and if not, when the organisation intends to do so.
- Contact details of the Company staff with whom the Information Regulator can liaise for further information or clarification

Where specific information of the Information breach is not yet available, the Company should send an interim notification comprising a brief description of the incident.

Notifications made by organisations or the lack of notification, as well as whether organisation has adequate recovery procedures in place, will affect the Information Regulator's decision(s) on whether an organisation has reasonably protected the personal Information under its control or possession.

Responding to an Information Breach

INFORMATION BREACH MANAGEMENT PLAN

Upon being notified of an Information breach, the Information Breach Team should immediately activate the Information breach & response plan.
The Company's Information breach management and response plan is:

1. Confirm the Breach.
2. Contain the Breach.
3. Assess Risks and Impact.
4. Report the Incident.
5. Evaluate the Response & Recovery to Prevent Future Breaches.

CONFIRM THE BREACH

- The Information Breach Team (IBT) should act as soon as it is aware of an Information breach.
- Where possible, it should first confirm that the Information breach has occurred.
- It may make sense for the IBT to proceed to Contain the Breach based on an unconfirmed reported Information breach, depending on the likelihood of the severity of risk.

CONTAIN THE BREACH

The IBT should consider the following measures to Contain the Breach, where applicable:

- Shut down the compromised system that led to the Information breach.
- Establish whether steps can be taken to recover lost Information and limit any damage caused by the breach.
- Prevent further unauthorised access to the system.
- Reset passwords if accounts and / or passwords have been compromised.
- Isolate the causes of the Information breach in the system, and where applicable, change the access rights to the compromised system and remove external connections to the system.

ASSESS RISKS AND IMPACT

Knowing the risks and impact of Information breaches will help the company determine whether there could be serious consequences to affected individuals, as well as the steps necessary to notify the individuals affected.

Risk and Impact on Individuals

- How many people were affected? A higher number may not mean a higher risk but assessing this helps overall risk assessment.
- Whose personal Information had been breached. Does the personal Information belong to employees, customers, or suppliers? Different people will face varying levels of risk as a result of a loss of personal Information.
- What types of personal Information were involved? This will help to ascertain if there are risk to reputation, identity theft, safety and/or financial loss of affected individuals.
- Any additional measures in place to minimise the impact of an Information breach?

Risk and Impact on organisations

- What caused the Information breach? Determining how the breach occurred (through theft, accident, unauthorised access, etc.) will help identify immediate steps to take to contain the breach and restore public confidence in a product or service.
- When and how often did the breach occur? Examining this will help the Company better understand the nature of the breach.
- Who might gain access to the compromised personal Information? This will ascertain how the compromised Information could be used. Affected individuals must be notified if personal Information is acquired by an unauthorised person.
- Will compromised Information affect transactions with any other third parties? Determining this will help identify if other organisations need to be notified.

REPORT THE INCIDENT
The Company is legally required to notify affected individuals if their personal Information has been breached.

This will encourage individuals to take preventive measures to reduce the impact of the Information breach, and also help the Company rebuild consumer trust.

Who to Notify:

- Notify individuals whose personal Information have been compromised.
- Notify other third parties such as banks, credit card companies or the police, where relevant.
- Notify the Information Regulator.
- The relevant authorities (e.g.: police) should be notified if criminal activity is suspected and evidence for investigation should be preserved (e.g.: hacking, theft or unauthorised system access by an employee.)

When to Notify:

- Notify affected individuals immediately if an Information breach involves sensitive personal Information. This allows them to take necessary actions early to avoid potential abuse of the compromised Information.
- Notify affected individuals when the Information breach is resolved.

How to Notify:

- Use the most effective ways to reach out to affected individuals, taking into consideration the urgency of the situation and number of individuals affected (e.g.: media releases, social media, mobile messaging, SMS, e-mails, telephone calls).
- Notifications should be simple to understand, specific, and provide clear instructions on what individuals can do to protect themselves.

What to Notify:

- How and when the Information breach occurred, and the types of personal Information involved in the Information breach.
- What the Company has done or will be doing in response to the risks brought about by the Information breach.
- Specific facts on the Information breach where applicable, and actions individuals can take to prevent that Information from being misused or abused.
- Contact details and how affected individuals can reach the organisation for further information or assistance (e.g. helpline numbers, e-mail addresses or website).

EVALUATE THE RESPONSE & RECOVERY TO PREVENT FUTURE BREACHES

After steps have been taken to resolve the Information breach, the Company should review the cause of the breach and evaluate if existing protection and prevention measures and processes are sufficient to prevent similar breaches from occurring, and where applicable put a stop to practices which led to the Information breach.

Operational and Policy Related Issues:

- Were audits regularly conducted on both physical and IT-related security measures?
- Are there processes that can be streamlined or introduced to limit the damage if future breaches happen or to prevent a relapse?
- Were there weaknesses in existing security measures such as the use of outdated software and protection measures, or weaknesses in the use of portable storage devices, networking, or connectivity to the Internet?
- Were the methods for accessing and transmitting personal Information sufficiently secure, e.g.: access limited to authorised personnel only?
- Should support services from external parties be enhanced, such as vendors and partners, to better protect personal Information?

- Were the responsibilities of vendors and partners clearly defined in relation to the handling of personal Information?
- Is there a need to develop new Information-breach scenarios?

Resource Related Issues:

- Were sufficient resources allocated to manage the Information breach?
- Should external resources be engaged to better manage such incidents?
- Were key personnel given sufficient resources to manage the incident?

Employee Related Issues:

- Were employees aware of security related issues?
- Was training provided on personal Information protection matters and incident management skills?
- Were employees informed of the Information breach and the learning points from the incident?

Management Related Issues:

- How was management involved in the management of the Information breach?
- Was there a clear line of responsibility and communication during the management of the Information breach?

Consequences of failing to comply:

We take compliance with this policy very seriously. Failure to comply puts both the employee and the Company at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.