Integrity Academy

PROTECTION OF PERSONAL INFORMATION POLICY

2016

Protection of Personal Information Policy (POPI)

Objective

The objective of this policy is to protect the information assets of Integrity Academy and its associated companies against threats, be it internal or external, whether with intent or accidental. This is necessary to ensure business continuation, curbing of losses and maximising of business opportunities.

This policy sets the standard for suitable protection of personal information in Integrity Academy. It provides the principles regarding the right for individuals to privacy and reasonable protection of personal information.

Scope

The policy is applicable to Integrity Academy, Associated Service Providers, their sole owners, key persons, representatives and other personnel in Integrity Academy. The sole owners, key personnel and management of Integrity Academy are eventually responsible for proper control of information security.

Integrity Academy's Information Control Officer

The responsibilities of Integrity Academy Group Information Officer (Johann Cloete) are as follows:

- The development and updating of this policy;
- Ensuring that this policy is supported with applicable documentation and procedural instructions;
- Assuring that documentation is relevant and kept up to date;
- Communicating the content of the policy, and consequential updating, to the relevant managers, representatives, personnel and associates concerned.

The sole owners, key personnel, representatives and personnel of Integrity Academy are obliged to comply with the provisions of this policy. Any deviations from this policy or breach thereof or incidents that may relate to such a possibility, must be reported to the Information Officer.

External individuals, involved in information technology under contract to Integrity Academy, will be subjected to the same information security policy as applicable to Integrity Academy. A separate contract will have to be signed confirming commitment to the policy and will include assurance that security measures are in place when personal information is processed.

Core Principles

The sole owners, key personnel, representatives as well as personnel of Integrity Academy are committed to the following principles:

- Integrity Academy will always maintain and develop reasonable protective measures against risks such as loss, unauthorised access, destruction, use, alteration or revelation of personal information.
- Integrity Academy will at all times comply with restrictions and other requirements applicable to the international transfer of information.

Integrity Academy upholds the requirements of the legislation on POPI and maintains an approach of transparency of operational procedures that control collection and processing of personal information.

- Integrity Academy is committed to comply with all applicable regulatory requirements related to the collection and processing of personal information.

- Integrity Academy undertakes to collect personal information in a legal and reasonable way and to process the personal information obtained from clients only for the purpose for which it was obtained in the first place.
- Processing of personal information obtained from clients will not be undertaken in an insensitive or wrongful way that can intrude on the privacy of the client.
- Integrity Academy undertakes not to request or process information related to race, religion, medical situation, political preference, trade union membership, sexual certitude or criminal record. Integrity Academy will also not process information of juveniles.
- Integrity Academy will ensure that correct and sufficient information is on record of its clients. Non relevant information will be removed. Only the latest information related to the training process will be recorded.
- Information will be directly obtained from the client.
- Integrity Academy also undertakes not to provide any documentation to a third party or service provider without the consent of the client except where it is necessary for the proper execution of the service as expected by the client, in compliance with the education provided, with the proviso that Integrity Academy will at all times ensure that the third party also complies with the stipulations and requirements of the POPI legislation as well as when documents are requested by institutions as prescribed by law.
- Integrity Academy is compelled to keep effective record of personal information and undertakes not to keep information for a period longer than that prescribed by the relevant educational legislation. Information will be destroyed at the end of the prescribed period in such a way that it cannot be reconstructed.
- Integrity Academy will provide the necessary security of data and keep it in accordance with prescribed legislation.
- Should information be lost, that is not under the control of Integrity Academy anymore, it will immediately be brought to the attention of the client and the regulator.
- In the event of data loss, the client will receive sufficient information to restrict possible risk that may result from the loss.
- Clients may at all times inquire about information kept and may also request the removal or destruction of information which is not relevant anymore.
- Integrity Academy will ensure that all service providers and other role players involved, comply with the expectations of the POPI legislation of 2013.
- The management of Integrity Academy give the assurance that representatives and staff understand the requirements and expectations of the act and comply with the content thereof and that training will take place on an ongoing basis.
- Integrity Academy's policy regarding private information will continuously be updated to comply with legislation, thereby ensuring that personal information will be secure.

Monitoring

The management as well as the information officer of Integrity Academy, are responsible for the implementation, administration and supervision of this policy. This function includes the provision of supporting guidelines, standardised operational procedures, notices, applicable documents and processes.

The sole owner, key personnel, representatives and staff of Integrity Academy will be trained to be conversant with their functions regarding the regulatory requirements, policy and guidelines related to the protection and control of personal information. The Facilitators, Assessors and Moderators of Integrity Academy will undertake periodic revision and auditing to ensure compliance with the policy, guidelines and the application of the principle of privacy of information.

Operational controls

Integrity Academy will implement suitable operational controls to ensure privacy of information in compliance with this policy and the regulatory requirements. These control measures will comprise of:

- Allocation of responsibilities for information security;
- Incident reporting and management;
- User ID inclusion or removal;
- Information security training and education;
- Data backup.

Implementation

This policy is implemented by the Management, Facilitators, Assessors, Moderators and staff of Integrity Academy. All stakeholders namely shareholders, directors, key personnel, representatives and staff of Integrity Academy as well as the Facilitators, Assessors, Moderators' assigned with the duty to collect and process personal information, must comply with the requirements of the policy.

Non-compliance to this policy will lead to disciplinary action such as a possible change of mandate or dismissal.

Signed on this 30th day of March 2016

Johann Cloete

Managing Director: Integrity Academy (Pty) Ltd

Tel: 012-348 1098

IMPLEMENTATION CHECKLIST

Companies can assess the amount of preparation needed to ready themselves for the implementation of the Protection of Personal Information Bill ("POPI") by considering the following minimum requirements:

1.	Audit the processes used to collect, record, store, disseminate and destroy personal information: in particular, companies must ensure the integrity and safekeeping of personal information in their possession or under their control. They must take steps to prevent the information being lost or damaged, or unlawfully accessed.	
2.	Define the purpose of the information gathering and processing: personal information must be collected for a specific, explicitly defined and lawful purpose that is related to a function or activity of the company concerned.	
3.	Limit the processing parameters: the processing must be lawful and personal information may only be processed if it is adequate, relevant and not excessive given the purpose for which it is processed.	
4.	Take steps to notify the 'data subject': the individual whose information is being processed has the right to know this is being done and why. The data subject must be told the name and address of the company processing their information. In addition, he or she must be informed as to whether the provision of the information is voluntary or mandatory.	
5.	Check the rationale for any further processing: if information is received via a third party for further processing, this further processing must be compatible with the purpose for which the data was initially collected.	
6.	Ensure information quality: the company processing the information must make sure the information is complete, accurate, up to date and not misleading.	
7.	Notify the information Protection Regulator: when the POPI is enacted and a Regulator established, organisations processing personal information will have to notify the Regulator about their actions.	
8.	Accommodate data subject requests: the POPI allows data subjects to make certain requests, free of charge, to organisations holding their personal information. For instance, the data subject has the right to know the identity of all third parties that have had access to their information. A data subject can also ask for a record of the information concerned.	
9.	Retain records for required periods: personal information must be destroyed, deleted or 'de-identified' as soon as the purpose for collecting the information has been achieved. However, a record of the information must be retained if an organisation has used it to make a decision about the data subject. The record must be kept for a period long enough for the data subject to request access to it.	
10.	Cross border data transfer: there are restrictions on the sending of personal information out of South Africa as well as on the transfer of personal information back into South Africa. The applicable restrictions will depend on the laws of the country to whom the data is transferred or from where the data is returned, as the case may be.	