RELATIONSHIP BETWEEN PRIVACY CONDITIONS AND INFORMATION SECURITY

Information Security (IS) is critical in ensuring the protection of personal information, especially with growing reliance placed on Information and Communication Technologies (ICT) to enable key business processes.

The table below defines the IS controls and how they are associated with privacy conditions in the Protection of Personal Information Act ("POPI Act"). The controls are based on leading practice as well as regulatory guidelines/ codes and provides a reference framework for implementing IS controls that align with requirements of the POPI Act.

POPI condition	POPI condition summary	Related IS controls
Accountability	1. Responsible parties must ensure that the conditions of the POPI Act are complied with.	• Established IS roles and responsibilities (organisation of IS and appropriate oversight from board-level). • Creation, embedment, enforcement and review of IS policies (e.g. acceptable use, mobile device policies, user access, information breach management policies). • Compulsory IS training and awareness. • Independent risk reviews of IS environment on a periodic basis. • Certification against ISO 27000 series or internationally recognised security standards.
Processing limitation	2. Personal information may only be processed in a fair and lawful manner, with the consent of persons providing their personal information.	• Data classification to support record retention, access management, user activity restrictions. • Inventory of information assets to support record discovery, maintenance and destruction. • Record retention procedures aligned with organisational retention requirements. • Procedures to manage disposal of media/ IT assets. • Appropriate Identity and Access Governance (IAG) controls are implemented, enforced and reviewed. • Security relating to systems collecting and storing personal information and consent/ preference. • System test environments use of anonymised data.
Purpose specification	3. Personal information may only be processed for specific and legitimate purposes.	
Further processing limitation	4. Personal information may only be processed if it is in line with the original purpose. Alternatively, consent must be obtained from the person for further processing	
Information quality	5. Organisations must put reasonable measures in place to ensure the quality of personal information they process.	• Formal data governance structure established. • Input validation controls implemented on systems involved in the collection of personal information. • Record retention procedures aligned with organisational retention requirements. • Database/ system cleanups are performed

POPI condition	POPI condition summary	Related IS controls
		periodically to identify redundant and inaccurate information. • Information backups are completed and secured as required to ensure availability and integrity of information. • Formal change control procedures and restrictions manage changes to systems or software.
Openness	6. Organisations must keep formal record of the personal information they process	• Formal and up-to-date inventory of information assets is maintained • Event logs are maintained, monitored and safeguarded. • Security and Privacy incident management procedures.
Security safeguards	7. Organisations must ensure that reasonably practical controls are in place to ensure the safeguarding of personal information they process. This includes: 8. Ensuring confidentiality, integrity and availability of information 9. Appropriate management of third parties that process personal information on behalf of the organisation 10. Appropriate information breach management and notification procedures	• Physical security controls are in place to protect information assets (e.g. locked cabinets, access controlled offices). • Vulnerability management (detective, preventative and corrective controls). • Appropriate Identity and Access Governance (IAG) controls are implemented, enforced and reviewed. • Mobile Device Management policies and procedures are implemented, enforced and reviewed. • Removable media management policies and procedures. • Procedures in place to manage disposal of Media/ IT assets. • Data Leakage Prevention (DLP) techniques • Security and Privacy incident management procedures. • Encryption on end-user devices and on operational level (static and moving information). • Third parties are appropriately managed (including signing of contracts, due diligence checks, security assurance).
Data subject participation	11. Persons must have the ability to request access to their personal information and to update, delete/destroy their personal information held by an organisation	• Formal and up-to-date inventory of information assets is maintained (electronic and IT assets) • Security relating to systems collecting and storing personal information and consent/ preference.

NOTE: IS controls may apply to a number of POPI conditions.

NOTE: implementation of the controls, policies and procedures listed in this document does not guarantee compliance with local or international privacy legislation. Organisations should align privacy related security controls with their information risk assessment, strategic objectives and the regulatory requirements applicable to their country, industry or organisation.