Protection of Personal Information (POPI) Compliance Reference Card

SOPHOS
Security made simple.

The POPI Act sets forth eight conditions for the lawful processing of personal information. These conditions address how organizations demonstrate accountability for ensuring they respect the privacy of individuals in South Africa. The Act regulates how this information is collected, stored, processed, and shared. Although the Act was signed into law in 2013 and certain sections of the Act went into effect in 2014, these effective sections pertained to the establishment and appointment of the Information Regulator. Once the sections of the Act that place obligations on organizations to ensure the lawful processing of personal information begin, organizations will have one (1) year following that date to comply with the Act's provisions. POPI Condition 7 on "Security Safeguards" includes security measures that responsible parties must comply with to ensure the integrity and confidentiality of personal information. Sophos products can help address the security requirements required for customers' POPI compliance program.

REQUIREMENT	SOPHOS PRODUCT	HOW IT HELPS
Boundary defense	Sophos XG Firewall	Provides all the latest advanced technology to protect your network from botnets, hacks, and advanced threats with Advanced Threat Protection, IPS, sandboxing, Web and Email Protection. Stops data-stealing attacks at your network perimeter with Synchronized Security that works side-by-side with endpoint protection to automatically identify and isolate compromised systems.
Malware protection	Sophos Central	Endpoint Protection, Server Security, and Intercept X modules on Sophos Central integrate innovative technology like malicious traffic detection with real-time threat intelligence to help prevent, detect and remediate threats with ease. Sophos Email uses real-time threat intelligence to detect and block 99% of unwanted email at the gateway, and our anti-spam engine catches the rest – including the latest phishing attacks, malicious attachments, and snowshoe spam. Sophos Mobile delivers Enterprise Mobility Management (EMM) and security for mobile devices, helping ensure sensitive data is safe, devices are protected, and users are secure. Sophos Mobile Security for Android provides leading antivirus, ransomware, and unwanted app protection for Android devices. Sophos Clean, a part of Intercept X, removes malicious code and registry keys created by malware in addition to cleaning the malware files after an infection.
	Sophos XG Firewall	Monitors and blocks malware infections and executables from accessing your website, and integrates up-to-date threat intelligence on malicious sites from Sophos. Sophos Sandstorm, optional cloud-sandbox technology, can be fully integrated into these Sophos security solutions to provide an extra layer of security. Sandstorm inspects and blocks executables and documents containing executable content before the file is delivered to the user's device.
	Sophos for Virtual Environments	Protects virtual servers and desktops from malware.

Data loss prevention	Sophos Central	Intercept X keeps your endpoints secure from the latest data-stealing malware and ransomware.
		Endpoint Protection Advanced detects unauthorized data distribution through administrator defined DLP policies.
		Sophos Secure Workspace (Sophos Mobile) encrypts documents within a secure container on a mobile device managed with Sophos Mobile. Sophos Secure Workspace can dynamically encrypt content sent to cloud-based storage services and applications. It enforces device encryption and monitors compliance relative to encryption policy.
	Sophos SafeGuard Enterprise	Manages encryption of devices and data on Windows, macOS, and mobile devices. SafeGuard can manage BitLocker and FileVault full disk encryption, as well as always-on encryption for files stored on hard disks, USB sticks, cloud storage, file shares, memory cards, and CDs/DVDs. All data encrypted with SafeGuard remains encrypted as files move across the network.
	Sophos XG Firewall	Allows for policy-based encryption for VPN tunnels, protecting data in transit.
		Sophos SPX encryption provides encryption both in transit and at rest. SPX encryption is able to dynamically encapsulate email content and attachments into a secure encrypted PDF to ensure compliance.
Data access control	Sophos XG Firewall	Offers controlled access to data based on the need to know with Sophos' patented Layer 8 user-identity technology that governs all firewall polices and reporting, enabling next-gen control over applications, web surfing, bandwidth quotas, and other network resources by user/group.
		Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
	Sophos SafeGuard Enterprise	Authenticates users for access to specific protected devices, files, and/or folders with the use of user- or group-specific keys. Supports multi-factor authentication, tokens, and smart cards for user authentication.
	Sophos Central	Protects privileged and administrator accounts with advanced two-factor authentication.
		Keeps access lists and user privileges information up to date. Provides procedures to ensure that access rights are revoked if individuals no longer meet the conditions to receive access (e.g., because they change position or leave the company).
		Sophos Secure Email and Sophos Secure Workspace in Sophos Mobile store content on mobile devices securely with AES-256 encryption. Access to the content in the apps can be restricted based on device compliance rules, time, Wi-Fi, or geo-location.
Audit and logs	Sophos SafeGuard Enterprise	Provides detailed logging of all access attempts.
	Sophos Central	Sophos Mobile creates detailed log events of all malicious activity on mobile devices, helping to identify suspicious activity that may try to access sensitive data.
	Sophos XG Firewall	Controls remote access authentication and user monitoring for remote access, and logs of all access attempts.
	All Sophos products	Generates security event logs that can be integrated into a centralized monitoring program for incident detection and response.

Specifications and descriptions subject to change without notice. Sophos disclaims in full all warranties and guarantees. This document and the information in it do not constitute legal advice. Customers are solely responsible for compliance with all laws and regulations, and should consult their own legal counsel for advice regarding such compliance.

SOPHOS