SOPHOS

Protection of Personal Information (POPI) Act Compliance Reference Card

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, the act came into force on July 1, 2020, with a one-year grace period for all South African entities to become compliant.

POPIA Condition 7 on "Security Safeguards" includes security measures that responsible parties must comply with to ensure the integrity and confidentiality of personal information. This document maps how Sophos solutions help to address the Security Safeguards requirements as part of a customer's efforts to comply with the POPI Act.

Specifications and descriptions are subject to change without notice. Sophos disclaims all warranties and guarantees regarding this information. The use of Sophos products alone does not guarantee legal compliance. The information in this document does 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.

REQUIREMENT	SOPHOS SOLUTION	HOW IT HELPS
Identify internal and external risks to personal information	Sophos XDR	Detect and investigate across endpoint, server, firewall, and other data sources. Get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail when needed. The Sophos Data Lake allows to quickly answer business critical questions, correlate events from different data sources and take even more informed action.
	Sophos Managed Detection and Response (MDR)	Proactively hunt threats 24x7 and neutralize even the most sophisticated threats with our managed detection and response services backed by an elite team of threat hunters and response experts who take targeted actions on your behalf.
	Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
	Sophos Cloud Optix	Scans cloud resources for security misconfigurations, profiling any alerts by risk level to help teams focus on the priority areas, and provide detailed remediation guidance to fix those issues.

Establish and maintain appropriate safeguards against the identified risks to personal information	Sophos Firewall	Enables role-based administration for delegating secure network security management; blocks traffic, services, ports and protocols except those explicitly allowed and defined as appropriate and necessary for the organization. Supports flexible multi-factor authentication options including directory services for access to key system areas. Includes IPS, APT, AV, sandboxing with deep learning, and web protection to monitor and block malicious, anomalous, and exploitive traffic from inbound or outbound access. Sophos Sandboxing, optional cloud-sandbox technology, inspects and blocks executables and documents containing executable content before the file is delivered to the user's device.
	Sophos Intercept X Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease across all devices and platforms.
	Sophos Cloud Optix	Establishes guardrails to prevent, detect, and remediate accidental or malicious changes in network configuration, network traffic, resource configuration, and user behavior or activities.
	Sophos Mobile	A rich set of device management capabilities keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices. Flexible compliance rules monitor device health and flag deviation from desired settings.
	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
	Sophos XDR	Detect and investigate across endpoint, server, firewall, and other data sources. Get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail when needed. The Sophos Data Lake allows to quickly answer business critical questions, correlate events from different data sources and take even more informed action.
	Sophos Wireless	Offers visibility into wireless network health and clients connecting to the network. With visibility into potential threats, such as rogue APs, insight into clients with compliance or connectivity issues and advanced diagnostics, identifying and troubleshooting issues is quick and easy.
	Sophos Managed Detection and Response (MDR)	24/7 monitoring of the environment plus investigation and neutralization of malicious activities secures against data loss through adversarial activities.
	Sophos ZTNA	Validates user identity, device health, and compliance before granting access to resources.
Protect against data stealing and other malware	Sophos Intercept X Sophos Intercept X for Server	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease across all devices and platforms. Includes rollback to original files after a ransomware or master boot record attack. Provides forensic-level remediation by eradicating malicious code as well as eliminating nasty registry key changes created by malware.
	Sophos Cloud Optix	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
	Sophos Email Sophos Firewall	Uses real-time threat intelligence to detect and block unwanted email at the gateway, and our anti-spam engine catches the rest – including the latest phishing attacks, malicious attachments, and snowshoe spam.
	Sophos Firewall	Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network. Delivers advanced protection from the latest drive-by and targeted web malware, URL/Malicious site filtering, Web Application Filtering, Cloud-based filtering for offsite protection.
	Sophos Sandboxing	Complements Sophos web and email security products and Sophos Firewall by inspecting and blocking executables and documents containing executable content before the file is delivered to the user's device.
	Sophos Intercept X for Mobile	Detects malicious and potentially unwanted applications installed on Android devices using Intercept X deep learning technology alongside intelligence from SophosLabs global research team. Integration with Microsoft Intune allows administrators to build conditional access policies, restricting access to applications and data when a threat is detected.

	Sophos Managed Detection and Response (MDR)	Sophos MDR continuously monitors signals from across the security environment, including network, email, mobile, identity, endpoint and more, enabling us to quickly and accurately detect potential cybersecurity events. Anomalous behaviors and code use are detected, investigated, and correlated to identify malicious activities and enable us to quickly neutralize the event.
	Sophos Rapid Response Service	Get incredibly fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
Manage personal information consistent with the organization's risk strategy to protect confidentiality, integrity, and availability of information	Sophos Firewall Sophos Intercept X Sophos Intercept X for Server	Data Leakage Prevention (DLP) capabilities in Sophos products can detect sensitive data like credit or debit card numbers and can prevent leaks of such information via email, uploads, and local copying.
	Sophos Email Sophos Firewall	Leverages Sophos SPX encryption to dynamically encapsulate email content and attachments into a secure encrypted PDF.
	Sophos Firewall	User awareness across all areas of our firewall governs all firewall policies and reporting, giving user-level controls over applications, bandwidth, and other network resources. Supports flexible multi-factor authentication options including directory services for access to key system areas. Allows for policy-based encryption for VPN tunnels, protecting data in transit.
	Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
	Sophos Mobile	A rich set of device management capabilities keeps sensitive business email and documents protected on mobile devices – even for users working with personal devices. Flexible compliance rules monitor device health and flag deviation from desired settings.
	Sophos Wireless	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos-managed networks and hotspots.
	Sophos Cloud Optix	Public cloud security benchmark assessments proactively identify storage services (e.g. Amazon S3), hard drive snapshots, and databases without encryption enabled, or with public access enabled and ports exposed. Guided remediation then instructs the administrator on how to protect these services and data at rest.
	Synchronized Security feature in Sophos products	Synchronized Security allows Sophos Firewall and Intercept X endpoint protection to work together to identify, isolate and clean up devices that have been compromised, preventing them from leaking confidential data. When the threat is neutralized and there is no risk of lateral movement, network connectivity is restored.
	Sophos Managed Detection and Response (MDR)	24/7 monitoring of the environment plus investigation and neutralization of malicious activities secures against data loss through adversarial activities.
Generate alerts when personal information is accessed or modified without authorization	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
	Sophos Managed Detection and Response (MDR)	Sophos MDR continuously monitors signals from across the security environment, including network, email, mobile, identity, endpoint and more, enabling us to quickly and accurately detect potential cybersecurity events. Anomalous behaviors and code use are detected, investigated, and correlated to identify malicious activities and enable us to quickly neutralize the event.
	Sophos Rapid Response Service	Get incredibly fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
	Sophos Cloud Optix	Scans cloud resources for security misconfigurations, profiling any alerts by risk level to help teams focus on the priority areas, and provide detailed remediation guidance to fix those issues.
	Sophos XDR	Goes beyond the endpoint, pulling in rich network, email, cloud, and mobile data sources to give you an even broader picture of your cybersecurity posture with the ability to drill down into granular detail when needed. With data from each product flowing into the Sophos Data Lake you can quickly answer business critical questions, correlate events from different data sources and take even more informed action.

Ensure user identity-based access to the network and network services based on users' roles and functions	All Sophos products	Sophos' user-identity-based policy technology allows user-level controls over network resources and other organization assets.
	Sophos Firewall	Supports flexible multi-factor authentication options including directory services for access to key system areas. Facilitates two-factor authentication for VPN connections, with granular RADIUS/TACACS integration.
	Sophos Cloud Optix	Adopt the principle of least privilege across public cloud environments with Sophos Cloud Optix, Cloud Security Posture Management solution. The SaaS based service connects disparate actions with Sophos AI to pinpoint unusual access patterns and locations to cloud provider consoles in near real time to identify credential misuse or theft. It includes an IAM visualization tool that provides a complete map of IAM relationships and allows teams to quickly and easily identify over-privileged access and create right-sized IAM policies before they are exploited in cyberattacks.
	Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
	Sophos Switch	Allows network access control that enables you to authenticate users using LDAP, MAC address, or other authentication methods to connect to a network. This prevents unauthenticated users and devices from gaining access to your LAN.
Ensure event logs recording user activities, exceptions, faults, and information security events are produced, kept, and regularly reviewed	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
	Sophos Firewall	Allows real-time insights into network and user events, quick and easy access to historical data, and easy integration with third-party remote management and monitoring tools (RMMs).
	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.
	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
	Sophos Managed Detection and Response (MDR)	Sophos MDR detects and investigates suspicious events from across the full security environment to identify threats and appropriate response activities. Data is collected across endpoint, network, identity email, and more, and then correlated using powerful AI tools, threat intelligence and human expertise to identify impact and response.
	Sophos XDR	Detect and investigate across endpoint, server, firewall, and other data sources. Get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail when needed. The Sophos Data Lake allows to quickly answer business critical questions, correlate events from different data sources and take even more informed action.
Identify the source of a data breach and the procedure to follow to neutralize such a breach	Sophos XDR	Detect and investigate across endpoint, server, firewall, and other data sources. Get a holistic view of your organization's cybersecurity posture with the ability to drill down into granular detail when needed. The Sophos Data Lake allows to quickly answer business critical questions, correlate events from different data sources and take even more informed action.
	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls–stopping advanced attacks.
	Sophos Managed Detection and Response (MDR)	Sophos MDR includes full incident response, delivered by a 24/7 team of response experts. Once an incident is remediated, Sophos MDR performs full root cause analysis which enables the environment to be hardened and response plans and strategies to be updated to incorporate learnings.
	Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.

Continually update the safeguards in response to new risks or deficiencies in previously implemented safeguards	Sophos Intercept X Sophos Intercept X for Server	Consistently looks at reported false positives and false negatives to ensure the product is being continuously improved. It integrates a deep learning malware detection model that can scale to hundreds of millions of training samples and can 'memorize' the entire observable threat landscape as part of its training process. It is regularly trained by our SophosLabs team to stay up to date over time.
	SophosLabs	Delivers the global threat intelligence advantage with Sophos' state-of-the-art big data analytics system that efficiently processes millions of emails, URLs, files, and other data points analyzed each day. This data, along with our extensive experience, enables us to develop new definitions, detect entire classes of threats, and even new variants. And, Live Protection and Live Anti-spam offer the data and expert analysis from SophosLabs in real time.
	Sophos Managed Detection and Response (MDR)	Sophos MDR includes full incident response, delivered by a 24/7 team of response experts. Once an incident is remediated, Sophos MDR performs full root cause analysis which enables the environment to be hardened and response plans and strategies to be updated to incorporate learnings.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK

2022-12-13 RC-NA (PS)

SOPHOS