ISO/IEC 27001:2013

SOPHOS

ISO 27001 is an international standard published by the International Standardization Organization (ISO). It describes how to manage information security in a company. It was written by the world's top experts in the field of information security and provides methodology for the implementation of information security management in an organization. The focus of ISO 27001 is to protect the confidentiality, integrity, and availability of a company's information. The latest revision of this standard was published in 2013 and its full title is now ISO/IEC 27001:2013. The standard can be implemented in any kind of organization, profit or non-profit, private or state-owned, small or large.

Note: ISO/IEC 27001 is split into 11 sections, plus Annex A. The sections 0 to 3 are introductory, describing the standard, and are not mandatory for organizations to implement. Sections 4 to 10 set the requirement for information security system and must be implemented by an organization if it wants to be compliant with the standard. Many of these sections highlight policies, planning, and procedures at the organization level, which are outside of the scope of this document. This document discusses Annex A that contains 114 security controls or safeguards grouped into 14 sections. The document maps out how Sophos security can support organizations to meet the security controls in Annex A. This document is not a replacement for ISO 27001.
To get the standard, visit the ISO website: http://www.iso.org.

CONTROL	DESCRIPTION	SOPHOS SOLUTION	HOW IT HELPS
A.6 ORGANIZATION OF INFORMATION SECURITY			
A.6.1.2 Segregation of duties	**Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.**	All Sophos products	Sophos' user-identity based policy technology allows user level controls over network resources and other organization assets.
A.6.2.1 Mobile device policy	**A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.**	Sophos Mobile	Provides enterprise mobility and security management capabilities for mobile devices, including security and device policies. Flexible compliance rules monitor device health and can automatically deny access to sensitive data in case of a compromised device. Emails and documents can be stored in the secure and encrypted Sophos Container and accessed with the Sophos Secure Email and Sophos Secure Workspace apps. The Sophos Secure Workspace app secures sensitive data with AES-256 encryption, allowing a secure way to manage, distribute, and edit documents and view web content on mobile devices.

ISO/IEC 27001:2013

SOPHOS

CONTROL	DESCRIPTION	SOPHOS SOLUTION	HOW IT HELPS
A.6.2.2 Teleworking Policy	**A policy and supporting security measures shall be implemented to protect information accessed, processed, or stored at teleworking sites.**	Sophos XG Firewall SG UTM	Facilitates two-factor authentication for VPN connections, with granular RADIUS/ TACACS integration. Sophos SD-RED [SD-WAN Remote Ethernet Devices] extends a secure network to a remote location easily by establishing a secure, dedicated VPN tunnel.
		Sophos SafeGuard Encryption	Authenticates users for access to specific files/folders with the use of user- or group-specific keys for SafeGuard encryption.
A.7 HUMAN RESOURCE SECURITY			
A.7.3.1 Termination and change of employment responsibilities	**There should be a process that ensures access to information assets are removed at the time of termination.**	Sophos XG Firewall SG UTM	User awareness across all areas of our firewall governs all firewall polices and reporting, giving user-level controls over applications, bandwidth, and other network resources.
		Sophos Central	Keeps access lists and user privileges information up-to-date. Procedures are in place 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).
A.9 ACCESS CONTROL			
A 9.1.2 Access to network and network services	**Users shall only be provided with access to the network and network services that they have been specifically authorized to use.**	Sophos XG Firewall SG UTM	User awareness across all areas of our firewall governs all firewall polices and reporting, enabling next-gen control over applications, web surfing, bandwidth quotas, and other network resources by user/group.
		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).

ISO/IEC 27001:2013

SOPHOS

CONTROL	DESCRIPTION	SOPHOS SOLUTION	HOW IT HELPS
		Sophos Mobile	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 health, compliance rules, time, Wi-Fi, or geo-location.
A 9.2.6 Removal or adjustment of access rights	**The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.**	Sophos XG Firewall SG UTM	User awareness across all areas of our firewall governs all firewall polices and reporting, giving user-level controls over applications, bandwidth, and other network resources.
		Sophos Central	Keeps access lists and user privileges information up-to-date. Procedures are in place 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).
A.9.2.3 Management of privileged access right	**The allocation and use of privileged access rights shall be restricted and controlled.**	Sophos Enterprise Console Sophos Central	Configurable role-based administration provides granular control of administrator privileges.
		Sophos Mobile	Role-based administration assures user privacy and appropriate credentials for altering compliance or device/data access.
		Sophos Firewall Manager	Centralized security management with extensive administrative controls; Role-based administration with change control and logging.

ISO/IEC 27001:2013

SOPHOS

CONTROL	DESCRIPTION	SOPHOS SOLUTION	HOW IT HELPS
A.10 CRYPTOGRAPHY			
A.10.1.1 Policy on the use of cryptographic controls	**A policy on the use of cryptographic controls for protection of information shall be developed and implemented.**	Sophos SafeGuard Enterprise	Encrypts data on Macs, Windows, and mobile devices. SafeGuard can manage BitLocker and FileVault full disk encryption, as well as always-on file encryption 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 Email Appliance Sophos XG Firewall SG UTM	Sophos SPX encryption provides encryption in transit and at rest. SPX encryption is able to dynamically encapsulate email content and attachments into a secure encrypted PDF to ensure compliance.
		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.
A.12 OPERATIONS SECURITY			
A.12.2.1 Controls against malware	**Detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.**	Sophos Intercept X Sophos Intercept X for Server	Anti-exploit, anti-ransomware, and deep learning malware detection protect endpoints from malicious executable code.
		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.
		Sophos Email on Central Sophos Email Appliance Sophos XG Firewall SG UTM	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.

ISO/IEC 27001:2013

SOPHOS

CONTROL	DESCRIPTION	SOPHOS SOLUTION	HOW IT HELPS
		XG Firewall	Includes IPS, APT, antivirus, sandboxing with deep learning, and web protection to monitor and block malicious, anomalous, and exploitive traffic from in-bound or out-bound access. Sophos Sandstorm, optional cloud-sandbox technology, inspects and blocks executables and documents containing executable content before the file is delivered to the user's device.
		Sophos Mobile	Delivers Unified Endpoint Management (UEM) and security management 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.
A.12.3.1 Information backup	**Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.**	Sophos Email on Central	In the event of third-party cloud email service provider outages, alerts are provided if mail can't be delivered to a server/service; email is then queued for delivery to ensures no email is lost, and access to that queued email is provided from a 24/7 emergency inbox inside the end user portal. Retry period for queued email is five days.
A.12.4.1 Event logging	**Event logs recording user activities, exceptions, faults and information security events shall be 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 XG Firewall	Controls remote access authentication and user monitoring for remote access, and logs all access attempts.
		Sophos SafeGuard Enterprise	Provides detailed logging of all access attempts.
		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.

ISO/IEC 27001:2013

SOPHOS

CONTROL	DESCRIPTION	SOPHOS SOLUTION	HOW IT HELPS
A.12.4.3 Administrator and operator logs	**System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.**	All Sophos products	All administrative actions are logged and available for reporting and audits.
A.12.5.1 Installation of software on operational systems	**Procedures shall be implemented to control the installation of software on operational systems.**	Sophos XG Firewall SG UTM Sophos Web Gateway	Allows user-based policy control over applications, websites, categories, and traffic shaping (QoS). Synchronized Application Control in XG Firewall identifies all networked applications in the environment running on Sophos-managed endpoints. User-based application policies enable custom-tailored application control to be added to any user, group, or network policy with the option to also apply traffic shaping.
		Sophos Intercept X	Endpoint Protection application control policies restrict the use of unauthorized applications.
		Sophos Intercept X for Server	Server Lockdown allows only trusted whitelisted applications and associated files to run.
A.12.6.2 Restrictions on software installation	**Rules governing the installation of software by users shall be established and implemented.**	XG Firewall	Visibility and Control over thousands of applications via customizable policy templates with granular controls based on category, risk, technology, or other undesirable characteristics (P2P apps, IMs, games and other harmful software); fully automated application security with pre-defined policy templates for commonly used enterprise applications/software packages; Synchronized Application Control in XG Firewall identifies all networked applications in the environment running on Sophos-managed endpoints. Full list of controlled software/applications.
		Sophos Mobile	Monitor devices for jailbreaking and side-loading of applications and deny access to email, network, and other resources if device is not in compliance with policy.

ISO/IEC 27001:2013

SOPHOS

CONTROL	DESCRIPTION	SOPHOS SOLUTION	HOW IT HELPS
A.13 COMMUNICATIONS SECURITY			
A.13.1.1 Network controls	**Networks shall be managed and controlled to protect information in systems and applications.**	XG 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.
		Sophos Mobile	Integration with Sophos UTM and other UTMs provides integrated and consistent security and compliance enforcement for mobile devices accessing the network and other services.
		Sophos Intercept X Sophos Intercept X for Server	HIPS, deep learning, anti-exploit, anti-adversary, and malicious traffic detection combine to proactively detect malicious behaviors occurring on the host.
A.13.2.1 Information transfer policies and procedures	**Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.**	Sophos Email Appliance Sophos XG Firewall SG UTM	Sophos SPX encryption provides encryption in transit and at rest. SPX encryption is able to dynamically encapsulate email content and attachments into a secure encrypted PDF to ensure compliance.
		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	Encrypts data on Macs, Windows, and mobile devices. SafeGuard can manage BitLocker and FileVault full disk encryption, as well as always-on file encryption 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 SG UTM	Allows for policy-based encryption for VPN tunnels, protecting data in transit

ISO/IEC 27001:2013

SOPHOS

CONTROL	DESCRIPTION	SOPHOS SOLUTION	HOW IT HELPS
A.13.2.3 Electronic messaging	**Information involved in electronic messaging shall be appropriately protected.**	Sophos Email Appliance Sophos XG Firewall SG UTM	Sophos SPX encryption provides encryption in transit and at rest. SPX encryption is able to dynamically encapsulate email content and attachments into a secure encrypted PDF to ensure compliance.
		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	Encrypts data on Macs, Windows, and mobile devices. SafeGuard can manage BitLocker and FileVault full disk encryption, as well as always-on file encryption 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.
A.16 INFORMATION SECURITY INCIDENT MANAGEMENT			
A.16.1.2 Reporting information security events	**Information security events shall be reported through appropriate management channels as quickly as possible.**	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
		Sophos XG Firewall SG UTM	iView Reporting provides intelligent, centralized reporting and analytics across multiple firewalls or sites; easy monitoring and analysis of security risks across entire network; convenient backup and long-term storage for security information.
A.16.1.5 Response to information security incidents	**Information security incidents shall be responded to in accordance with the documented procedures.**	Synchronized Security feature in Sophos products	Shares telemetry and health statu,s enabling coordinated isolation, detection and malware remediation across servers, endpoints, and firewalls, stopping advanced attacks.
		Sophos Intercept X Sophos Intercept X for Server	Get the root cause analysis of an attack with complete visibility on the how and where of the attack, along with recommendations on what your next steps should be.

ISO/IEC 27001:2013

SOPHOS

CONTROL	DESCRIPTION	SOPHOS SOLUTION	HOW IT HELPS
A.16.1.7 Collection of evidence	**The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.**	Sophos Intercept X Sophos Intercept X for Server	Get the root cause analysis of an attack with complete visibility on the how and where of the attack, along with recommendations on what your next steps should be.
A.17 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT			
A.17.2.1 Availability of information processing facilities	**Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.**	Synchronized Security feature in Sophos products	High availability with active-active load balancing or active-passive fail-over and WAN link balancing lets you easily double your performance when you need it.
A.18 COMPLIANCE			
A.18.1.4 Privacy and protection of personally identifiable information	**Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.**	Sophos Intercept X Sophos Intercept X for Server	Data loss prevention policies prevent misuse and distribution of predefined data sets.
		Sophos Email Appliance Sophos XG Firewall SG UTM	SPX encryption dynamically encapsulates email content and attachments into a secure encrypted PDF to help support compliance.
		Sophos SafeGuard Enterprise	Complete data protection solution that is effective across multiple platforms and devices, including mobile and traditional endpoints. Protect data at rest with full disk encryption. Location-based file encryption protects data in motion and follows the file wherever it may go – for example, via email, uploaded to cloud storage, or copied to removable devices. Application-based (synchronized) encryption encrypts data by default as soon as it is created.

ISO/IEC 27001:2013

CONTROL	DESCRIPTION	SOPHOS SOLUTION	HOW IT HELPS
		Sophos Mobile	Delivers mobile data protection when integrated with SafeGuard Enterprise to enable seamless access to encrypted content on mobile devices. The secure Sophos Container for email, documents, and content makes sure that protected data stays separate and can be locked down or wiped.

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

2020-04-09 RC (PS)

SOPHOS