The Ohio Data Protection Act

The Ohio Data Protection Act (Senate Bill 220) went into force in November 2018. The Act provides a legal safe harbor to businesses that implement a specified cybersecurity program by providing compliant businesses with an affirmative defense to tort actions brought under Ohio law or in Ohio courts. To be eligible for this affirmative defense, the business must create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information and restricted information, and that reasonably conforms to an industry-recognized cybersecurity framework. Some examples of acceptable frameworks include NIST, HIPAA/HITECH, FedRAMP, GLBA, CIS Controls, FISMA, ISO 27000 Family, and PCI DSS.

The particular design of the cyber security program will vary by business, taking into account a business's size and complexity, nature and scope of activities, sensitivity of information, cost and availability of tools to improve security, and resources available to the business. Thus, a smaller business may face different threshold requirements for implementing an effective cyber security regime than a larger business.

Sophos products can support your efforts to build a robust cybersecurity program that aims at protecting the security and confidentiality of information, protecting the security and integrity of information against anticipated threats or hazards, and protecting against unauthorized access to and acquisition of the information that may result in identity theft or other fraud. For more Sophos solutions that can reinforce your regulatory compliance efforts, please visit: sophos.com/compliance.

Specifications and descriptions are subject to change without notice. Sophos disclaims all warranties and guarantees regarding this information. 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.

SOPHOS

Security goal from cybersecurity framework	Sophos solution	How it helps
Requirement 1: Protect the security and confidentiality of the information		
Install and maintain a firewall configuration to protect data.	Sophos Firewall	Includes next-gen IPS that offers advanced protection from hacks and attacks using a uniform signature format backed by SophosLabs. Besides traditional servers and network resources, it also helps to identify and protect users and applications on the network. 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.
	Sophos Intercept X Sophos Intercept X for Server	Enforces web, data, and device policies to allow only authorized applications to be run, devices to be connected and data to be distributed.
	Sophos Cloud Optix	Proactively identifies an unsanctioned activity, vulnerabilities, and misconfigurations across AWS, Azure, and GCP. Complete cloud edge firewall solution includes IPS, ATP, and URL filtering and lets you deploy several network security products at once to protect your hybrid cloud environments against network threats.
	Sophos Managed Detection and Response (MDR)	Threat hunting experts monitor and correlate signals from across the network, identifying and investigating suspicious activities. Sophos NDR generates high caliber, actional signals across the network infrastructure to optimize cyber defenses.
Ensure integrity, confidentiality, and availability of data	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.
	Sophos Firewall Sophos Intercept X Sophos Intercept X for Server	Data Leakage Prevention (DLP) capabilities in Sophos products can detect sensitive data and can prevent leaks of such information via email, uploads, and local copying.
	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.
	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	Continuously validates user identity, device health, and compliance before granting access to applications and data.
	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.
	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 Email	Granular control of data breach prevention policies, including multi-rule policies for groups and individual users with seamless integration of encryption. Create custom CCLs using Sophos Content Control Lists or customize out of the box templates for specific CCLs. Choose from a variety of policy outcomes including block, drop attachment, quarantine as well as log and continue mode.
Ensure business continuity and disaster recovery planning	Sophos Firewall	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.

Security goal from cybersecurity framework	Sophos solution	How it helps
	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)	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 Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
	Sophos Intercept X Sophos Intercept X for Server	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.
Requirement 2: Protect against any anticipated threats or hazards to the security or integrity of the information		
Identify and assess internal and external cybersecurity risks that threaten the security and integrity of stored 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.
	All Sophos Products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
	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 Rapid Response Service	Provides incredibly fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
	Sophos Cloud Optix	Cloud Optix enables organizations to design public cloud environments to meet Amazon Web Services, Microsoft Azure, and Google Cloud Platform security best practice standards and maintain them. This agentless service continually monitors public cloud resources, providing the visibility to proactively identify unsanctioned activity, vulnerabilities, and misconfigurations.
	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 Mobile	Monitor mobile devices for jailbreaking and side-loading of applications. Deny access to email, network, and other resources if device is not in compliance with policy.
Secure transmitted data	Sophos Firewall	Allows for granular rule-based traffic control to specific ports and services at perimeter ingress and egress points, and can control remote access authentication and user monitoring at the perimeter.
	Sophos Wireless	Creates dynamic encrypted Wi-Fi sessions, protecting information in transit on Sophos-managed networks and hotspots.
	Sophos Email	Encrypt messages and add a digital signature to verify sender identity with S/MIME, or select from customizable encryption options, including TLS encryption, attachment and message encryption (PDF and Office), or add-on full web portal encryption.
Respond to identified or detected Cybersecurity Events to mitigate any negative effects	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 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.

Security goal from cybersecurity framework	Sophos solution	How it helps
	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 Managed Detection and Response (MDR)	24/7 detection, investigation and neutralization of suspicious activities by human experts enables us to identify and stop exploitation of vulnerabilities by adversaries. Sophos X-Ops experts keep operators up-to-date on the latest threat and vulnerability developments.
	Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
	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.
Requirement 3: Protect against unauthorized access to and acquisition of the information that is likely to result in a Material risk of identity theft or other fraud to the individual to whom the information relates		
Identify and authenticate access to system components	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.
	Sophos Central Device Encryption	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
	Sophos Central	Protects privileged and administrator accounts with advanced two-factor authentication. Keeps access lists and user privileges information up to date.
	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.
	All Sophos products	Generate security event logs that can be integrated into a centralized monitoring program for incident detection and response.
	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	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.

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

SOPHOS