Sophos Information Security Program Overview

August 2026

Table of Contents

Overview

Sophos defends more than 600,000 organizations worldwide with an AI-native platform and expert-led services. The same discipline Sophos applies to defending our customers is applied to our own organization. Our Information Security Program is built on globally recognized standards, governed from the Board of Directors through to operational teams, and validated by independent assessment.

Sophos' security program protects our confidential information, intellectual property, and information systems as critical assets. The purpose of this overview is to provide insight into how Sophos safeguards the confidentiality, integrity, and availability of customer data and the systems that process it.

Governance and Accountability

Sophos manages information security through defined layers of accountability, separating those who operate controls, those who oversee them, and those who independently assess them.

First Line: Operational Ownership.

Control owners across the organization design and operate security controls within their respective functions. Every business area is responsible for implementing and maintaining security requirements that apply to their systems and processes. Information security is a shared responsibility: every Sophos employee and contractor is accountable for upholding the Information Security Policy within their area.

Second Line: The Corporate Security Function.

Led by the Chief Information Security Officer (CISO), the Cybersecurity function owns the security strategy, maintains the policies and standards, operates security monitoring and response, and ensure controls meet industry and regulatory requirements. The CISO has a direct escalation path to the Chief Executive Officer.

Third Line: Independent Assurance.

The Internal Audit function operates independently to evaluate control effectiveness, identify gaps, and recommend improvements, providing objective assurance the program operates as designed.

The Security Organization

The Cybersecurity function led by the CISO is organized into specialized teams, each with a defined charter and remit. Together they cover the full lifecycle of security: from how software is designed and built, through how the platform is monitored and defended, to how risk is governed. The teams operate on a shared-responsibility model: they provide expertise, tooling, and standards as a force multiplier to engineering, product, and corporate teams, who retain ownership of their own systems.

Application Security.

Helps engineering teams build secure software across the development lifecycle. Operates static code analysis, software composition analysis, threat modeling, and security reviews. In addition, the team runs the bug bounty and vulnerability triage programs, sets secure-coding standards, and measures software-security maturity against industry standards.

Architecture and Infrastructure Security.

Secures the design of Sophos infrastructure and platforms. Conducts security architecture reviews and infrastructure-as-code analysis, secures cloud environments and CI/CD pipelines, and designs the shared security services such as hardware security modules and secrets management.

Internal Detection and Response.

Sophos' security operations center, defending the organization by identifying threats and responding to incidents. Conducts proactive threat research and intelligence-driven threat hunting; engineers and tunes detections that surface malicious activity; operates continuous alert triage and full incident-response lifecycle, from detection through containment, forensic investigation, recovery, and post-incident review.

Offensive Security (Red Team).

Tests Sophos' defenses from an adversary's perspective. Delivers penetration testing for products and corporate systems, continuous external attack-surface and dark-asset monitoring, organization-wide red team and tabletop exercises, and adversary attack-path mapping.

Security Education and Evangelism.

Builds security awareness and capability across Sophos. Delivers new-hire security fundamentals, ongoing awareness and phishing-simulation programs, secure-coding training for engineers, and runs the Security Champions program that embeds security expertise within teams throughout the organization.

Trust and Assurance (Governance, Risk, and Compliance).

Operationalizes compliance and security assurance across the organization. Establishes and monitors security compliance controls against framework requirements; owns the certifications and standards program that enables market access; runs the customer assurance program that provides transparency into Sophos' security posture; and identifies, assesses, and mitigates third-party and supplier risk.

Policy and Standards

The Sophos Information Security Policy establishes the principles that direct the program. It is supported by a structured set of standards and procedures that translate those principles into consistent, repeatable practice. Policy supporting documents are owned by an accountable team, written to make a specific expectation concrete, and reviewed regularly. The Information Security Policy is reviewed at least annually, approved by leadership, and made accessible to all employees; supporting standards are owned and maintained by the relevant teams.

Secure Product Development

Standards in this category govern how security is embedded throughout the software development lifecycle, from design and architecture through coding, composition, and release.

- **Secure Software Development Life Cycle Standard.** Embeds security across every phase of software development, from planning through release and maintenance.
- **Application Security Requirements Standard.** Establishes baseline security requirements built into products from the outset.

- **Application Security Training Standard.** Ensures developers are trained to write secure code and recognize common attack patterns.
- **Threat Model Standard.** Standardizes threat modelling to identify and mitigate attack scenarios early in design.
- **Source Code Management Standard.** Protects source code from unauthorized modification or disclosure.
- **Static Application Security Testing Standard.** Requires static code analysis to identify security flaws before code is released.
- **Software Composition Analysis Standard.** Identifies and remediates risks in third-party and open-source components.
- **Third-Party Software Use Standard.** Governs the lawful, secure, and maintained use of third-party and open-source software.
- **Container Security Requirements Standard.** Defines security requirements for containerized environments.
- **Code Signing Standard.** Enables customers to verify the authenticity of software released by Sophos.
- **SBOM Publishing Standard.** Establishes how software bills of materials are produced and made available on request.
- **Product Security Tooling Standard.** Ensures application security tooling meets consistent requirements across teams.
- **Supplier Security Standard.** Requires suppliers to meet Sophos security obligations, ensuring consistent product security regardless of component origin.

Vulnerability and Incident Response

Standards in this category govern how Sophos identifies, triages, and remediates security vulnerabilities in its products, and how it communicates them to customers and the public.

- **Vulnerability Response Standard.** Defines how identified vulnerabilities are triaged and remediated.
- **Vulnerability and Application Security Risk Measurement Standard.** Establishes consistent measurement and prioritization of security risk.
- **CVE Assignment Standard.** Governs the assignment of official vulnerability identifiers (CVEs).
- **Public Response Standard.** Defines consistent handling of publicly reported vulnerabilities.
- **Security Advisory Standard.** Ensures security advisories are accurate, clear, and consistent.

Monitoring and Operations

Standards in this category ensure Sophos environments generate sufficient visibility for security monitoring and that operational systems are consistently inventoried and secured.

- **Security Logging Standard.** Requires logging sufficient to support timely incident investigation.
- **Security Review Standard.** Defines when security reviews occur and the quality standard they must meet.
- **Service Operation Standard.** Ensures services are segregated and customer data remains within dedicated production systems.
- **Self-Managed System Standard.** Ensures systems outside central IT remain inventoried and secured.

Identity, Access, and Encryption

Standards in this category define how access to systems and data is authorized and authenticated, and how information is protected through cryptography throughout its lifecycle.

- **Access Management Standard.** Establishes consistent rules for access authorization and permission management.
- **Authentication Standard.** Defines secure identity verification and credential handling.
- **Cryptography Standard.** Governs the use of approved cryptographic algorithms and protocols.
- **Key Management Standard.** Defines secure handling of keys and secrets throughout their lifecycle.
- **Key Infrastructure Standard.** Establishes disciplined management of certificates and public key infrastructure.

Data Protection

Standards in this category govern how Sophos classifies, handles, retains, and disposes of information in alignment with its privacy and security obligations.

- **Data Classification and Sharing Standard.** Classifies information by sensitivity and defines corresponding handling and sharing requirements.
- **Data Retention and Destruction Standard.** Establishes retention periods and secure destruction requirements.

The framework additionally includes the standards governing day-to-day operations and the wider organization, including the Acceptable Use Policy, Asset Management Standard, Human Resources and Personnel Security Standard, Physical Security Standard, Mobile Device Security Standard, Corporate and Cloud Network Security Standards, Corporate and Product Change Management Standards, Business Continuity and Disaster Recovery Standard, Incident Response Plan, Supplier Risk Management Standard,

AI Standard, and the Policy and Governance Document Management Standards that maintain the framework itself.

Security Controls

Sophos has established controls across the following domains to protect customer data and the systems that process it.

Access Management.

Role-based access is enforced under the principle of least privilege. Single sign-on and multi-factor authentication are applied wherever technically feasible. Access is reviewed regularly and revoked promptly on role change or departure.

Data Protection.

Customer data is encrypted in transit and at rest using industry-standard protocols. A Data Classification and Sharing Standard governs handling by sensitivity, supported by a key management standard and defined retention and disposal processes.

Network Security.

A Zero Trust model governs access to network resources, systems, and applications, with safeguards to prevent interference between internal networks and external devices or applications.

Security Monitoring and Response.

Continuous security monitoring feeds a dedicated security information and event management (SIEM) system, operated by the Cybersecurity operations team. A documented incident response process governs reporting, classification, containment, investigation, remediation, stakeholder communication, and post-incident review.

Vulnerability Management.

Regular vulnerability scanning is supplemented by third-party assessments and penetration tests conducted at least annually. Sophos monitors CVE sources, scores findings using CVSS, and prioritizes remediation accordingly.

Supplier Risk Management.

Security due diligence is performed before any third party with access to customer data is engaged, supported by required agreements and non-disclosure agreements, with ongoing review of critical suppliers.

Personnel Security.

Background screening is completed before access is granted. Policy acknowledgement is mandatory, and security awareness training is delivered at hire and annually thereafter.

Business Continuity and Disaster Recovery.

Continuity and recovery plans are developed from a business impact analysis, stored securely, and tested at least annually. Backups are aligned to recovery objectives and data criticality.

Secure Development.

A defined secure development lifecycle governs application development, incorporating secure coding aligned to industry standards, mandatory peer code review, and segregation of development, test, and production environments.

Change Management.

A formal change management framework defines change classification, documentation, approval workflows, and emergency-change procedures. All production changes are documented and approved prior to implementation.

Risk Management.

Critical assets and threats are identified, assessed for likelihood and impact, and addressed through tracked mitigation. Significant risks are reported to management and recorded in a maintained risk register.

Customer Data Handling

Sophos handles customer data with care, transparency, and defined purpose.

- **Encryption.** Customer data is encrypted in transit and at rest.
- **Classification and Ownership.** The Data Classification and Sharing Standard establishes handling and control requirements by sensitivity, and assigns accountable owners responsible for safeguards and retention.
- **Retention.** Sophos' approach to data collection and retention is set out in the Sophos Privacy Policy.
- **Sub-Processors.** Sophos maintains a current list of third-party sub-processors that may process customer data on its behalf. Each is subject to the supplier risk management process, which includes review of audit reports and security questionnaires to confirm an appropriate level of security assurance before engagement. The authorized list is published in the Sophos Trust Center.

Security Assurance

Independent certification is how a security program is verified rather than merely asserted. Each certification Sophos holds reflects an independent auditor's examination of how the organization operates, measured against a globally recognized standards for protecting the confidentiality, integrity, and availability of information. Certifications are maintained through recurring assessment, ensuring they reflect current operating practice rather than a single point in time.

Sophos maintains a comprehensive portfolio of certifications and attestations and aligns its program to the regulatory frameworks applicable to its customers worldwide. To ensure the information remains accurate and current, the complete list is maintained in a single authoritative location rather than reproduced here.

The current list of certifications, attestations, and supported regulatory frameworks is available at:

sophos.com/en-us/trust/business-certifications