

Sophos 2022 Transparency Statement

U.K. Modern Slavery Act (2015)

This Sophos 2022 Transparency Statement (the Statement) is made following Section 54 of the Modern Slavery Act 2015 (the Act)ⁱ, and other related legislation, as it applies to Sophos Limited, a commercial organization that does business in the UK and worldwide, supplying goods and services having a total annual turnover of £36 million or more, and all entities in the Sophos Group global structure (together *Sophos* or the *Group*). This peer-reviewed Statement sets out the steps that have been taken during the fiscal year ending 31 March 2022 (FY22) to ensure that modern slavery is not taking place in the Sophos Supply Chain or in any part of Sophos business.

This Statement has been signed by Kris Hagerman, Chief Executive Officer, on behalf of Sophos Group Companies and has been published on the [homepage of the Group's website](#) and on the [Sophos Trust Center](#).

Sophos continues to prioritize the establishment and implementation of effective systems and controls described in the [Sophos Modern Slavery Policy](#) (the Policy), originally adopted in 2016 and updated during the past fiscal year, reflecting Sophos' commitment to acting legally, ethically, transparently, and with high integrity in all business dealings, relationships, vendor, and third-party partnerships where individuals are employed by them. The Policy sits alongside the [Sophos Anti-Corruption Policy](#) the [Sophos Whistleblowing Policy](#). Further, Sophos' compliance with the U.K. Modern Slavery Act is a comprehensive platform under which Sophos also meets the broader demands of similar legislation, such as the *California Transparency in Supply Chain Act of 2010*ⁱⁱ, certain U.S. federal regulations, and *The Commonwealth Modern Slavery Act 2018, Australia*ⁱⁱⁱ.

Sophos Statement covers the following topics:

- A. Our Business Model-** Sophos' product capabilities, partnerships, and global reach.
- B. Sophos Risk Assessment-** Measurements applied to respond to potential risks in the environments where Modern Slavery may exist.
- C. Our Governance and Policies-** A description of operational policies, actions taken and measurements in place to ensure compliance with the Act.
- D. Sophos Standard Operating Procedures-** Actions required from our supply chain and steps undertaken by the business for recruiting.
- E. Training** - An explanation of the training systems used to promote awareness amongst Sophos team members.
- F. Our Monitoring and Performance Review-** A description of the steps and indicators used to evaluate risk in our supply chain and in our business.

During FY22, Sophos focused on training, monitoring, and ongoing enforcement of its systems and processes to maintain high standards, which has improved Sophos ability to see, understand, and effectively manage the risk of modern slavery in any form.

A. Our Business Model

Sophos is a leading global provider of cybersecurity as a service through cloud-enabled, end-user, network, cloud, and email security solutions, offering organizations end-to-end protection against known and unknown cybersecurity threats through products and services that are easy to install, configure, update, and maintain. At the end of FY22, the number of customers supported reached more than 528,000. Sophos products are sold through its relationships with distributors and resellers, more than 55,000 partners around the world.

At the end of its FY22, Sophos had approximately 4,500 team members worldwide, including an office in the UK, many offices worldwide, and a few threat assessment labs, Sales, and product development centers around the world, including in Asia Pacific, Europe, the Middle East, North America, and South America.

The Sophos supply chain consists of many organizations comprised of hardware manufacturers, suppliers, logistic fulfillment centers responsible for product distribution, service vendors, as well as recruitment and employment agencies through which Sophos team members may be sourced (each a *Supplier*; collectively, the *Sophos Supply Chain*). Moreover, Sophos has close working relationships with and responsibilities to works councils in several jurisdictions, which represent the interests and rights of employees, including Sophos team members.

During FY22, Sophos saw significant growth in the number of its channel partners and end-users. As Sophos' business grows, we continue to find new and effective ways to understand the Group's forced labor risk, and we continue to adjust our compliance controls to ensure that any risk remains visible and managed.

B. Sophos Risk Assessment

Sophos faces modern slavery risks in two principal areas:

- 1) The Sophos Supply Chain and Suppliers located in jurisdictions outside the U.K.
- 2) The Sophos business enterprise, including employment, internal policies, and certain recruitment through agencies and third parties.

The formal process for identifying, evaluating, and managing significant risks faced by Sophos is overseen by the Board, along with the Group's Finance, Legal, and Compliance Teams. These Teams provide the business with a risk management framework, upward reporting of significant risks, Sophos policies, and standard operating procedures.

The potential for non-compliance with the Act is assessed as part of this risk management process. Sophos undertakes this risk assessment with input from external advisers; the assessment criteria applied include business function and geography, together with the principles set out by [Transparency International](#), [The Responsible Business Alliance Code of Conduct](#), and the [U.N. Global Coalition Against Corruption](#). During the reporting period, Sophos continued its adherence to the Responsible Business Alliance Code of Conduct, Version 7.0 (2021) (RBA Code of Conduct), particularly Section A.1., Freely Chosen Employment. [The Sophos Declaration to the RBA Code of Conduct](#) was signed by our CEO on 19 February 2021 and is published on the Group website.

Each Supplier is also assessed during the onboarding process and screened with the use of the Dow Jones Adverse media list. Suppliers must confirm they will comply with Sophos Modern Slavery Code of Conduct and complete the Slavery and Trafficking Risk Template (STRT) and the Conflict Minerals Reporting Template (CMRT). Current Group statistics show a 100% response from all Sophos Suppliers for completion of the Modern Slavery Code of Conduct, the Slavery and Trafficking Risk Template (STRT), and the Conflict Minerals Reporting Template (CMRT).

Both the STRT and the CMRT assess the Suppliers' actions under international standards, are verified by each Supplier each time submitted, and measure how they screen, prioritize, train, identify and manage risk, report, and have internal policies in place to govern against forced labor and to find appropriate mineral sources used in hardware products. These assessments are required from Suppliers every two years. For clarity, no Supplier is owned by the Group.

Sophos takes a two-pronged approach to risk identification: (i) a bottom-up approach at the business function level; and (ii) a top-down approach at the senior leadership team level. All identified risks are assessed against a pre-defined scoring matrix and prioritized accordingly. Any risks identified in the bottom-up approach deemed to be rated as higher risk are escalated in line with pre-defined escalation procedures for further evaluation.

C. Our Governance and Policies

The Board governing the Group has leadership responsibility for ensuring the Policy complies with the Group's legal and ethical obligations, and that all those under the control of the Group comply with the Policy.

The Board provides oversight regarding the implementation of the Policy and monitoring of risks and issues raised in connection with it. The Policy recognizes Sophos' responsibilities under the Act, its application to the Sophos Supply Chain, and places requirements on all persons working for Sophos in any capacity, including team members at all levels: directors, officers, agency workers, seconded workers, volunteers, interns, agents, contractors, external consultants, third-party representatives, and business partners.

During the period concerned, the Policy and Modern Slavery Code of Conduct have been revised to incorporate requirements regarding child labor in the workplace, and training has been provided to all team members. These revisions were reviewed and approved by the Board governing the Sophos Group. Following a peer review of the Sophos Modern Slavery Statement and the Sophos Modern Slavery Policy, Sophos revised its Policy to adopt key provisions of the United National Global Compact, to include prohibitions of child labor in the Policy.

The [Sophos Conflict Minerals Policy](#), implemented in 2020, also supports Sophos' commitment to reducing, if not removing, Modern Slavery in the Sophos Supply Chain. Sophos Supply Chain team members are responsible for reading, understanding, and enforcing this policy. 100% of these team members, including those in Product Management, Finance and Business Operations departments, have completed training on the Conflict Minerals Policy.

Any breach of the Policy by a Sophos team member would result in disciplinary action, and potential dismissal. Any breach of the Policy by a Supplier, vendor, or other third-party would result in a termination of the business relationship and further action depending on the circumstances.

All those subject to the Policy are encouraged to raise concerns about any suspicion of modern slavery in any part of our business, within the Sophos Supply Chain, or among any current or potential Suppliers or vendors, when they have any credible information about a policy violation or a prohibited practice. The [Sophos Whistleblowing Policy](#) provides a mechanism to enable team members and external entities, including third parties, to report matters of concern confidentially via the [Sophos Whistleblowing Portal](#), directly to their line manager, or to a designated HR manager. All such matters reported to the Whistleblowing Portal are investigated and evaluated until they are concluded. Sophos' Compliance Team has responsibility for adherence to the Policy and for investigating and evaluating Whistleblower complaints. Where appropriate, such matters are brought to the attention of Sophos' Senior Management Team and, where appropriate, to the Audit Committee of the Board. Consistent with the Sophos Whistleblowing Policy, Sophos is committed to ensuring no one suffers any detrimental treatment as a result of reporting in good faith their credible information of a policy violation or prohibited practice.

D. Sophos Standard Operating Procedures

Our Suppliers: We take the following actions with each Supplier:

- a. We inform all our new and renewed Suppliers in writing that we will not accept any form of labor exploitation in their business or in their supply chain, and we give them a copy of our Policy;
- b. All Suppliers are required to make a Sophos Modern Slavery Code of Conduct declaration stating that they are in full compliance with our Policy. This declaration includes the identification of all parties that supply products to our Supplier to ensure extended supply chain information is visible to Sophos and integrated into our management controls;
- c. Suppliers are required to complete an annual questionnaire, which includes Suppliers' identification of actions taken to build and maintain a socially responsible supply chain. This questionnaire was

adapted from the Social Responsibility Alliance (SRA) Slavery and Trafficking Risk Template (STRT);

- d. Suppliers must complete the Conflict Minerals Reporting Template (CMRT), a standardized reporting template developed by the Responsible Minerals Initiative (RMI);
- e. Suppliers have been asked to provide ISO 9001 and OHSAS 18001 certification to evidence actions they have undertaken for their organizations;
- f. We account for each step of our hardware manufacturing processes and know who is providing the hardware to us that we resell. This is performed by using BOMcheck, an industry-wide regulatory compliance tool which is offered by ENVIRON. BOMcheck identifies companies that are part of the Sophos extended supply chain that supply components for our hardware products, as well as our immediate Suppliers. Any anti-corruption or modern slavery changes for a specific Supplier will trigger an immediate review and business investigation, together with identifying specific risk indicators and categories;
- g. Our standard supply chain contract templates contain anti-slavery provisions which prohibit Suppliers and their team members and sub-suppliers from engaging in modern slavery;
- h. We conduct regular risk assessments of the Sophos Supply Chain. In cases of elevated risk, we may request Suppliers to provide a 'Statement of Compliance' on their actions to prevent slavery and to confirm that any concerns have been satisfactorily and promptly resolved;
- i. We undertake detailed due diligence when onboarding new distributors requesting that they have their own Policy regarding Modern Slavery or Human Trafficking. Otherwise, the new distributor must agree to comply with the Sophos Policy. The Policy is made available to our distributors during their onboarding process;
- j. In cases of high-risk, we also audit the Supplier and, as appropriate, we require them to take specific measures to ensure that the risk of modern slavery is significantly reduced. If slavery is identified in a business in the Sophos Supply Chain, Sophos will require immediate remedial action be taken, and appropriate support will be provided, to achieve the safest outcome for potential victims. Sophos expects its Suppliers to engage constructively and responsibly, and to remedy any issues promptly. Should the Supplier fail to resolve the situation to Sophos' satisfaction, their business relationship will be terminated;
- k. Should allegations of slavery in any part of the Sophos Supply Chain emerge, including from whistle blowers, Sophos will comprehensively investigate such allegations, and if any slavery is identified, will take immediate action as set out above.

Our Business: We take the following actions within Sophos:

- a. We ensure all team members have a written contract of employment and that they have not had to pay any direct or indirect fees to obtain work;
- b. We ensure team members are legally able to work in the country where they are recruited;
- c. We check the names and addresses of each team member (several people listing the same address may indicate high shared occupancy, often a factor for those being exploited);
- d. We provide information to all new recruits on their statutory rights including sick pay, holiday pay and any other benefits to which they may be entitled;
- e. We invest in the professional development, health, and wellbeing of Sophos team members, including Mental Health days, which occur throughout the fiscal year;

- f. We pay all Sophos team members in the UK at least the Living Wage (pro rata in the case of part-time team members; vacation students and interns are paid an allowance);
- g. If, through our recruitment process, we suspect someone is being exploited, our Human Resources Team will follow investigative and reporting procedures;
- h. We perform due diligence checks on any recruitment agency that we use to ensure that it is reputable and conducts appropriate checks on all team members they may supply to us.

E. Training

Mandatory training on Modern Slavery, Conflict Minerals, Anti-Corruption, and Whistleblowing is provided to all existing Sophos team members annually and to new joiners during onboarding. Training is accompanied by an online resource facility which is available to all Sophos team members. Refreshment of these materials is ongoing. Feedback is encouraged to improve the Policy and future updates of the training material for all Sophos team members.

F. Our Monitoring and Performance Review

Sophos engages an external compliance data provider on an ongoing basis to audit the Sophos Supply Chain and keep it under review. Together with our external compliance data provider, Sophos monitors the performance of the Policy, together with the [Sophos Anti-Corruption](#) and [Whistleblowing](#) Policies. Sophos maintains a watching brief on the compliance of all Suppliers through live monitoring tools. Any alert raised through this process will be subject to an internal review and where appropriate, an investigation of the Supplier will be undertaken.

During FY22, no material alerts were raised by our external compliance data provider concerning any Supplier, including recruitment agencies.

Indicators to Evaluate Risk.

Every endeavor is made to fully adhere to the requirements of the Modern Slavery Act 2015 in relation to our recruitment, employment, and internal policies. The following measures support this:

- i. Visibility and Management of the Sophos Supply Chain
 - a. Account for each step of our supply processes, and knowing who is providing goods and services to us;
 - b. Our level of communication and personal contact with the next link in our supply chain and their understanding of, and compliance with, our expectations.
- ii. Assessment, Code of Conduct, and Statement of Compliance
 - a. Number/percentage of new and existing Suppliers satisfactorily screened using risk assessment tools and/or self-assessment questionnaires, including risk scoring and categorization;
 - b. Number/percentage of Suppliers who have signed our Code of Conduct;
 - c. Number/percentage of Suppliers who have provided a satisfactory Statement of Compliance about their actions to prevent slavery, and any concerns have been satisfactorily and promptly resolved.
- iii. Reports on Concerns
 - a. Number of reported concerns of slavery (including if there were none);
 - b. Any material issues arising from implementation of the Policy were effectively escalated when the need arose;
 - c. All concerns raised as a result of audits or allegations were promptly followed-up and resolved;
 - d. How we responded to concerns raised or to issues found by screenings, assessments, or audits and how we worked with suppliers to implement corrective action plans.
- iv. Training and Awareness

- a. Number/percentage of relevant team members trained, informed, or completed mandatory training.

Sophos makes responsible sourcing decisions, develops plans to avoid brand damage, and complies with regulatory demands within the below legislation, among others:

- Modern Slavery Act 2015, United Kingdomⁱ
- California Transparency in Supply Chains Actⁱⁱ
- United States Federal Acquisition Regulations
- Trade Facilitation and Trade Enforcement Act of 2015^{iv}
- The Commonwealth Modern Slavery Act 2018, Australiaⁱⁱⁱ.

To ensure Sophos' actions expressed in its Modern Slavery Statement met all requirements laid out the Act, Sophos participated in a peer review facilitated by a trade association within its industry segment^v. Feedback from the reviews support Sophos in meeting these requirements, as well as providing further information about Sophos' actions that reduce and remove modern slavery in the Sophos Supply Chain.

All Suppliers reviewed were validated down to the family tree level. This indicates the number of entities that are contained in every Supplier's corporate structure.

Conclusion

Sophos' actions, essential to manage its compliance with the Act, continue to mature. Existing processes are in place to ensure that these tasks are kept under regular and effective review and that Sophos' performance under the Act is routinely and robustly measured.

This Statement is made following section 54(1) of the Act.

Dated: Sep 10, 2022


Kris Hagerman (Sep 10, 2022 14:45 GMT+2)

Kris Hagerman
Chief Executive Officer
Sophos Group Companies

ⁱ <https://www.legislation.gov.uk/ukpga/2015/30/contents/enacted>

ⁱⁱ https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersafety/sb_657_bill_ch556.pdf

ⁱⁱⁱ <https://www.legislation.gov.au/Details/C2018A00153>

^{iv} <https://www.cbp.gov/trade/forced-labor>; <https://www.govinfo.gov/app/details/PLAW-114pub1125>

^v techUK, <https://www.techuk.org/>