Incident Response Tabletop Exercise Service – Service Description

This Service Description describes Incident Response Tabletop Exercise Service ("**Service**"). All capitalized terms in this Service Description have the meaning ascribed to them in the Agreement (defined below).

This Service Description is part of and incorporated into, as applicable: (i) Customer's manually or digitally-signed agreement with Sophos covering the purchase of a Service subscription; (ii) if no such signed agreement exists, then this Service Description will be governed by the terms of the Sophos End User Terms of Use posted at https://www.sophos.com/legal (collectively referred to as the "**Agreement**"). To the extent there is a conflict between the terms and conditions of the Agreement and this Service Description, the terms and conditions of this Service Description will take precedence.

Notwithstanding anything to the contrary in the Agreement, Customer acknowledges and agrees that: (i) Sophos may modify or update the Service from time to time without materially reducing or degrading its overall functionality; and (ii) Sophos may modify or update this Service Description at any time to accurately reflect the Service being provided, and any updated Service Description will become effective upon posting to https://www.sophos.com/legal.

1.1 Overview

Sophos will provide Customer with an Incident Response Tabletop Exercise, which assembles primary stakeholders and uses a scripted incident scenario to practice incident response. The exercise facilitator releases information in a controlled manner that will guide the exercise, while each stakeholder describes their response as if it were a real incident. Incident Response Tabletop Exercise is an efficient way to familiarize Customer personnel with Incident Response practices and the exercise proactively tests existing response capabilities, including the validation of roles, responsibilities, coordination, and decision making. The Service is designed to improve Customer cybersecurity Incident Response capabilities and meet annual requirements often established via governance requirements.

1.2 Customer Obligations

Customer will perform the obligations listed below, and acknowledges and agrees that the ability of Sophos to perform the Service is contingent upon the following:

- Customer personnel are scheduled and available to assist as required for the Service(s).
- Customer will have obtained consent and authorization from the applicable third party, in form and substance satisfactory to Sophos, to permit Sophos to provide the Service if Customer does not own network resources such as IP addresses, Hosts, facilities or web applications.
- For on-site activities, Customer will provide a suitable workspace for Sophos personnel, and necessary access to systems, network, and devices.
- Replies to all requests are prompt and in accordance with the delivery dates established between the parties.
- Customer's scheduled interruptions and maintenance intervals allow adequate time for Sophos to perform the Service.
- Customer will provide to Sophos all required information (key personnel contact information, credentials, and related information) at least two (2) weeks before initiating the Service.

1.3 Scheduling

Sophos will contact a Customer-designated representative within five (5) business days after the execution of a Agreement to begin the Service Initiation activities described herein. These activities will ensure effective and efficient use of the Service.

Sophos will use commercially reasonable efforts to meet Customer's requests for dates and times to deliver the Service(s), taking into consideration Customer-designated downtime windows, Customer deliverable deadlines, and other Customer scheduling requests. Written confirmation of an agreed-upon schedule shall constitute formal acceptance of such schedule.

Once scheduling of any on-site work at Customer facility has been mutually agreed to, any changes by Customer to the on-site work within two (2) weeks of the on-site work to be performed will incur a $2,000 re-scheduling fee. This re-scheduling fee does not apply to work that does not require travel by Sophos.

1.4 Timeline

- On-site work will be performed Monday – Friday, 09:00 – 17:00 Customer's local time or similar daytime working hours.
- Remote work will occur Monday – Friday, 09:00 – 17:00 Customer's local time or similar daytime working hours.
- Work performed outside of the hours listed above, as requested or required by Customer, will incur additional service charges.

2 Service Details

The subsections below contain details about the Service and how it will be initiated.

2.1 Service Initiation

In preparation for an Incident Response Tabletop Exercise, Sophos will distribute a brief questionnaire to gather information and understand Customer goals and expectations prior to initiating the Service.

Information and insights collected through the questionnaire will be used to develop content for the Incident Response Tabletop Exercise, which will be held either remotely or on-site. Sophos may also request a brief scoping teleconference with relevant parties to discuss the scope and goals of the Incident Response Tabletop Exercise.

When the Service is assigned to a consultant, Sophos will collaborate with Customer to develop and customize the Incident Response Tabletop Exercise. Before the Service is performed, Customer will be allowed to review the proposed content to be used for the Incident Response Tabletop Exercise and request updates. Sophos can adjust the content as needed.

2.2 Service Scope

A standard Incident Response Tabletop exercise includes one (1) three-hour session and a conference room debriefing for up to fifteen (15) contributing participants (non-contributing observers are allowed at Customer's discretion).

2.3 Service Methodology

Throughout the Service delivery process, Sophos will deploy a Review and Research, Facilitate and Evaluate methodology:

Review and Research:

- Sophos will start by gathering requirements from the Customer point of contact(s) and conducting a comprehensive document review to understand the Customer's exercise goals and objectives.
- Critical systems, data, and personas will be identified to ensure the scenario aligns with the Customer's cybersecurity concerns.
- Sophos may collect information about the Customer's environment or conduct reconnaissance to gain insight into potential vulnerabilities and threat vectors to create a relevant and effective exercise.

The development of threat-informed scenarios will incorporate the most recent cybersecurity threats and industry best practices. Sophos will collaborate with the Customer to determine the scenario type that best meets their requirements, which may include ransomware, business email compromise, insider threats, DDoS attacks, data breaches, and more.

Facilitate and Evaluate:

Whether the exercise is conducted remotely or on-site, an experienced Sophos facilitator will guide the participants through the scenario. Throughout the exercise, specific events and challenges will be introduced at designed intervals to test the participants' responses and decision-making under duress. Sophos will facilitate post-exercise discussions to evaluate actions taken, decisions made, and lessons learned. The Customer's capabilities to respond to incidents will be evaluated and recommendations for improvement provided.

2.4 Service Delivery

The subsections below contain information about how Service and support are delivered to Customer.

2.4.1 Delivery Coordination

Sophos will provide coordination for the Service(s) with appropriate communication and updates to the stakeholder community. The coordinator will oversee logistics for people, processes, and tools as well as timeline and meeting facilitation.

The scope of delivery coordination includes the following:

- Develop delivery timeline with Customer and with Sophos personnel
- Work with Customer to identify and address issues or concerns that impact service delivery
- Periodic, high-level updates on progress
- Confirm delivery and procure project sign-off

Services will be delivered from Customer’s site(s) and/or remotely from a secure location. Sophos and Customer will determine the location of the service(s) to be performed herein.

Sophos solely reserves the right to refuse to travel to locations deemed unsafe by Sophos or locations that would require a forced intellectual property transfer by Sophos. Sophos solely reserves the right to require a physical security escort at additional Customer expense to locations that are deemed unsafe by Sophos. Customer will be notified at the time that services are requested if Sophos refuses to travel or if additional physical security is required, and Customer must approve the additional expense before Sophos travel is arranged. In the event any quarantines, restrictions, or measures imposed by

governmental authority or Sophos restrict travel to any location, Sophos may at its election (i) deliver the Services remotely or (ii) postpone the Services until travel is permitted. If neither option (i) nor (ii) in the preceding sentence is feasible, Sophos may terminate the affected Services and provide Customer with a refund of any unused, prepaid fees.

2.5 Deliverables

Listed in the tables below are the standard deliverables for the Service. Sophos will work with Customer to determine appropriate specific deliverables, delivery method, and cadence.

Service	Deliverable(s)	Delivery Schedule	Delivery Method
Incident Response Tabletop Exercise	Incident Response Tabletop Exercise Report	Mutually agreed upon	Mutually agreed upon

2.5.1 Incident Response Tabletop Exercise Report

Following the facilitated scenario and debrief, Sophos will supply a detailed Incident Response Tabletop Exercise Report. This report will present risk-prioritized findings, and offer actionable recommendations to improve Incident Response practices. These findings and recommendations will help Customer increase their incident readiness, build cyber resilience and mitigate future cyber threats.

Standard Incident Response Tabletop Exercise Reports may include the following:

- List of participants and exercise goals
- Description of the exercise scenario(s)
- Findings and observations
- Areas for development and recommendations

2.6 Out of Scope

The information in Section 2 comprises the Sophos standard in-scope offering for the Service. Any other services or activities not specifically listed as in scope are out of scope.Sophos reserves the right to decline requests that:

- Are beyond the scope of the Service(s) described herein
- Are beyond the capability of Sophos to deliver within the contracted service levels
- Might violate legal or regulatory requirements

3 Service Fees and Related Information

See Sophos applicable Agreement for details, including the following:

- Billing and Invoicing
- Out-of-Pocket Expenses
- Services Term

3.1 Invoice Commencement

See the Service-specific Addendum incorporated herein by reference at

https://www.sophos.com/legal/-terms, as updated from time to time (the "Product Terms Page") or Agreement for information about invoice commencement. Provisions related to the term of the Service and payment terms within the Product Terms Page shall not apply to Customer's consumption of Services in case of purchases through a Sophos' reseller but instead shall be subject to Customer's agreement with its reseller.

3.2 Expenses

Customer agrees to reimburse Sophos, directly or indirectly (in case of purchases through an authorized reseller), for all reasonable and actual expenses incurred in conjunction with delivery of the Service.

These expenses include but are not limited to the following:

- Travel costs related to transportation, meals, and lodging to perform the Services, including travel to Customer location(s). Additionally, time spent traveling to/from Customer location(s) will be billed to Customer, up to eight (8) hours per day for each participating Sophos employee.
- Specific equipment necessary for delivering the Service.

Monthly fees for other purchased infrastructure to support service delivery (e.g., public cloud computing services) may apply, if Customer and Sophos agree that usage is necessary to complete Service delivery.

3.3 Term

The term of the Service is defined in the Agreement. Service will expire according to the Agreement provided that, if there is currently an in-progress delivery of the Service at the time of expiration, then the term shall automatically extend and expire upon completion of such in-progress delivery of the Service. During such extended term (if applicable), the terms and conditions of the Agreement shall be in full force and effect.

4 Additional Terms

4.1 On-site Services

Notwithstanding Sophos' employees' placement at Customer's location(s), Sophos retains the right to control the work of such employees. For international travel, on-site Services may require additional documentation, such as visas, visitor invitations, and related documentation, which may affect timing of the Services and reimbursable expenses.

4.2 Record Retention

Sophos will retain a copy of the Customer Reports in accordance with Sophos' record retention policy. Unless Customer gives Sophos written notice to the contrary prior thereto and subject to the provisions of the applicable Agreement and DPA, all Customer Data collected during the Services and stored by Sophos will be deleted within 30 days from issuance of the final Customer Report. If Customer or its authorized agent requests that Sophos retain Customer Data for longer than its standard retention policy, Customer shall pay Sophos' costs and expenses associated with the extended retention and storage of such Customer Data. Notwithstanding the foregoing, Sophos shall be entitled to retain Customer Data as necessary to comply with its own legal, regulatory, judicial, audit, or internal compliance requirements.

4.3 Compliance Services

Customer understands that, although Sophos' Services may discuss or relate to legal issues, Sophos does not provide legal advice or services, none of such Services shall be deemed, construed as or constitute legal advice and that Customer is ultimately responsible for retaining its own legal counsel to provide legal advice. Furthermore, any written summaries or reports provided by Sophos in connection with any Services shall not be deemed to be legal opinions and may not and should not be relied upon as proof, evidence or any guarantee or assurance as to Customer legal or regulatory compliance.