Fields Auto Group Compliance

Service Provider Risk Assessment

Questionnaire requested by **Bentley Orlando, BMW of Asheville, Colocation Facility, Fields BMW Lakeland, Fields BMW Northfield, Fields BMW of Daytona, Fields BMW South Orlando, Fields BMW Winter Park, Fields Cadillac Jacksonville, Fields Cadillac St. Augustine, Fields CJDR Asheville, Fields CJDR Glenview, Fields Collision Center Glenview, Fields Collision Center Orlando, Fields Collision Jacksonville, Fields Jaguar Land Rover Volvo Madison, Fields Jaguar Land Rover Volvo Waukesha, Fields Lexus Glenview, Fields Mazda of Asheville, Fields Motorcars Lakeland, Fields Motorcars Orlando, Fields Volvo Cars Madison, Fields Volvo Cars Northfield, Fields Volvo Cars Waukesha, Jaguar Asheville Authorized Service, Jaguar Jacksonville, Jaguar Madison, Jaguar Northfield, Jaguar Waukesha Authorized Service, Land Rover Asheville, Land Rover Jacksonville, Land Rover Madison, Land Rover Northfield, Land Rover Waukesha, Lexus of Jacksonville, Lexus of Orange Park, Mercedes-Benz of Asheville, Mercedes-Benz of Bourbonnais, Mercedes-Benz of Jacksonville, Mercedes-Benz of Orange Park, Mercedes-Benz of Orland Park, MINI of Glencoe, Orlando MINI, Porsche Jacksonville**.

Name of Person Completing This Questionnaire	Service Provider Name	Date Completed
Chris Roszak	Sophos Inc.	7/29/2024

1. Are you an employee or authorized representative of this vendor/company? Indicate the Person's Name in the comments.	Yes	Person's Name: Chris Roszak
2. Does your company offer software applications as part of its services?	Yes	Sophos offers a range of software applications as part of its services. These applications include antivirus, antimalware, firewall, web security, encryption, and identity management solutions. Sophos's software is known for its effectiveness in protecting against cyber threats and providing secure digital environments for businesses and organizations.
3. Is client data encrypted at rest and in transit? If not, why not?	Yes	"All data at rest is encrypted using volume-level encryption: storage volumes, object storage, and virtual drives of virtual machines. For sensitive customer data, we use field-level encryption within storage volumes using a per-field multi-part key. These parts are formed from several different locations, including a key management system. Each key is unique to every customer, and every field. Transport-level encryption is used to secure management communication between the client software and Sophos Central platform via certificates and server validation. And for corporate system we encrypt data at rest via Bitlocker and access to applications requires MFA authentication. For cloud assets we use Vault and AWS KMS as applicable."
4. Has your company experienced a data breach in the past 12 months that affected customers' personal information?	No	"Sophos has not experienced a breach that required notification to affected individuals under applicable breach laws. However, out of an abundance of caution, we have notified users in the following instances: https://www.sophos.com/en-us/security-advisories/2022-02-centrallogging https://community.sophos.com/support-portal/b/announcements/posts/support-portal-exposure-faq"
5. Does your company have insurance coverage for a data breach that may involve our customer information that your company acquires while doing business with us?	Yes	Sophos has Cyber Liability insurance coverage with AIG's Cyber Liability Insurance Program. This insurance provides coverage for costs associated with a data breach, including notification expenses, credit monitoring expenses, legal defense expenses, and business interruption expenses.
6. Does your company require security awareness training for all employees? If so, please answer how often it is provided in the comments section.	Yes	Based on our current process, all employees, contractors, and third-party resources that need access to Sophos network resources are required to complete the mandatory security onboarding training and acceptable usage policy training. This training is to be taken at the time of onboarding and on an annual basis.
7. Does your company monitor for the effectiveness of employee security training by testing your users with simulated attacks?	Yes	"Sophos does monitor the effectiveness of employee security training by testing our users with simulated attacks. This helps us identify areas where our employees may need additional training or resources to stay secure. We use a variety of tools and techniques to test our users, including phishing campaigns, and security awareness training. We also conduct regular security assessments to identify any vulnerabilities in our systems and infrastructure."

8. Does your company have a process for restricting access to customer files on a need-to-know basis?	Yes	Selected Sophos employees have access to the Production environment hosted in AWS for the purpose of typical system operations and maintenance. These employees have specific job functions and belong to Authorization groups, which grant them these privileges. However, at no time do they have access to customer information. Sophos Support personnel can access customer environments for a limited period of time upon customer requests – customers must manually select within their Central environment that Sophos Support is authorized to access their environment.
9. Do you have a written information security program?	Yes	"Sophos has a documented information security policy that exhaustively covers all areas pertaining to security. The Sophos Information Security policy is for internal use only and cannot be shared externally. Please see this link for the High-level Overview of the Sophos Security Policy: https://www.sophos.com/en-us/trust/high-level-security-policy-overview.aspx"
10. Does your company conduct annual risk assessments that assess electronic, physical, and administrative information safeguards?	Yes	"Sophos does conduct annual risk assessments to evaluate the security of our electronic, physical, and administrative information safeguards. These assessments are conducted by internal and external security professionals who assess our policies, procedures, and infrastructure to identify potential vulnerabilities and risks. Based on the results of these assessments, we develop and implement appropriate security measures to mitigate these risks and ensure the security of our customer's information. This includes measures such as encryption, firewalls, intrusion detection systems, employee training, and regular security audits. We also participate in industry-wide security standards and compliance programs such as ISO 27001, PCI DSS, and HIPAA to ensure that our security practices meet the highest industry standards."
11. Does your company have systems in place to securely dispose of documents that have personal identifiable information on them?	Yes	"Sophos has systems in place to securely dispose of documents that contain personal identifiable information (PII). We follow a strict process for destroying sensitive documents, including shredding them and then recycling the paper. We also use secure deletion software to ensure that any data on the documents is completely erased before they are disposed of. Our security team monitors the disposal process to ensure that it is carried out in a secure and compliant manner. In addition, we have policies and procedures in place to protect the confidentiality of PII during the storage and disposal process. Our employees are trained on these policies and procedures and are required to adhere to them at all times."
12. Does your company have systems in place to restrict access to files/documents containing customers personal information to those with proper authorization?	Yes	"Sophos use a combination of security measures, such as encryption, access controls, and identity and access management (IAM) systems, to ensure that only authorized individuals can access sensitive data. Our IAM systems allow us to define and manage user roles and permissions, which determine what users can access and do with our data. We also use two-factor authentication to add an extra layer of security to user accounts."
13. Does your company have due diligence processes and procedures for vetting subcontractors, including having them sign processing agreements that are compliant with applicable federal and state laws?	Yes	"Sophos has due diligence processes and procedures for vetting subcontractors, including having them sign processing agreements that are compliant with applicable federal and state laws. We require all subcontractors to comply with our data security standards and policies, and we conduct regular audits and assessments of our subcontractors to ensure that they are meeting these requirements. Our processing agreements require subcontractors to protect the privacy and security of our customer's data and to adhere to all applicable laws and regulations. We also require subcontractors to provide us with access to their data processing facilities and to allow us to conduct security assessments of their systems. If a subcontractor fails to meet our requirements or violates our processing agreements, we may take appropriate action, including terminating our relationship with them."
14. Has your company performed penetration testing of its systems within the past 12 months?	Yes	"We use a third-party penetration testing service to conduct these tests and to identify any vulnerabilities in our systems and infrastructure. The results of these tests are then reviewed by our security team and used to improve our security posture. We also conduct regular security assessments and audits to ensure that our systems and processes are compliant with industry standards and regulations. We do have a list of our recent Penetration Testing Engagements at this link: https://www.sophos.com/en-us/trust/security-testing"
15. Has your company conducted a vulnerability assessment of your systems within the past 6 months?	Yes	" Sophos has conducted a vulnerability assessment of our systems within the past 6 months. The results of these assessments are then reviewed by our security team and used to improve our security posture. We also conduct regular security assessments and audits to ensure that our systems and processes are compliant with industry standards and regulations."

Fields Auto Group Compliance

16. Does your company maintain end-of-life or unsupported operating systems or software? If so, are these systems used to manage or maintain customer data?	No	Sophos does not leverage EOL systems/applications for critical functions of the business or delivery of our services.
17. Does your company regularly patch or update systems and third-party software and monitor for noncompliance?	Yes	"Sophos regularly patches or updates systems and third-party software and monitors for noncompliance. We have a team of dedicated security professionals who monitor our systems and networks for any potential vulnerabilities and threats. We also use a variety of tools and technologies to detect and respond to security incidents. In addition, we have a compliance program in place that requires our employees to adhere to best practices for security and to follow our policies and procedures for securing our systems and data. We conduct regular audits and assessments of our compliance program to ensure that it is effective and up-to-date."
18. Does your company have a written incident response plan in the event of a security breach?	Yes	"Sophos has a written incident response plan in the event of a security breach. Our plan outlines the steps that we will take to identify and respond to a security incident, including notifying affected parties, containing the incident, and conducting a thorough investigation. We also have a team of trained security professionals who are responsible for implementing our incident response plan and for responding to security incidents. We conduct regular training and exercises to ensure that our team is prepared to handle any security incident that may occur. Please also see this link for additional information: https://www.sophos.com/en-us/trust/incident-response"
19. Does your company require users to create complex passwords with 9 characters or greater?	Yes	"Sophos requires users to create complex passwords with 9 characters or greater. This helps to ensure that our systems and data are protected from unauthorized access. We encourage users to use a combination of characters, including uppercase letters, lowercase letters, numbers, and symbols, to make their passwords even more secure. Additionally, users should not reuse passwords for different accounts and should change their passwords regularly."
20. Does your company prohibit shared logins?	Yes	"Sophos prohibits shared logins. This helps to ensure that our systems and data are protected from unauthorized access. We encourage users to use a combination of characters, including uppercase letters, lowercase letters, numbers, and symbols, to make their passwords even more secure. Additionally, users should not reuse passwords for different accounts and should change their passwords regularly."
21. Does your company require multi-factor authentication to log into your systems?	Yes	Sophos requires multi-factor authentication to log into our systems.
22. Do you have an account lockout policy?	Yes	Sophos has an account lockout policy in place to prevent unauthorized access to our systems.

Date	Signature of Authorized Agent of Service Provider	Title
7/29/2024	Chris Roszak	Enterprise Sales Director

Submitted on July 29, 2024 at 12:39 PM by 73.72.150.55.