


THINK TRUTH. THINK COVENTBRIDGE GROUP.



Truth Package

The Global Leader in Full-Service Investigations

Table of Contents

Commitment to Trust.....	1
Cyber Security and your Data.....	1
Who is CoventBridge?.....	1
What is SmartPartner.....	1
Information in SmartPartner.....	1
Information Security	2
Information Security Management.....	2
Governance Risk and Compliance.....	2
Corporate and Operation Security	4
Identity and Access Management.....	4
Awareness and Training.....	4
Configuration Management.....	5
Security Operations.....	5
Security Incident Management.....	5
Business Continuity.....	6
SmartPartner Application Security.....	7
Infrastructure	7
Software Development Lifecycle	7
Encryption	7
Key Management.....	7
Authentication	7
Role-Based Access.....	7
Product Security Testing	7
Application Security Testing.....	7
OWASP Top 10	8
Appendices	8

Commitment to Trust

At CoventBridge, integrity and transparency are at the very core of our business. In order to establish a foundation of confidence and certainty with our partners, we've created this trust package describing all relevant security practices and documentation. We've compiled the information within this package to address the most common cyber security risk questions asked by potential business partners from a vendor risk management standpoint. If you have additional questions, please let us know.

Cyber Security and your Data

Before you can understand the information security requirements for mitigating risks associated with CoventBridge's access to your data, you should have an understanding of:

- What services your company uses CoventBridge for.
- The classification of the information CoventBridge will have access to (PII, PHI).
- How critical our service availability is to your business.
- The legal, regulatory, or contractual requirements of the information you're sharing with us.

At CoventBridge, we understand and take seriously the importance of your vendor risk management, and we're committed to being a faithful steward of the data you entrust with us.

Who is CoventBridge?

CoventBridge provides comprehensive, global investigative solutions. Led by an extensive network of experts backed by the latest technology, data protection, and legal expertise, we provide investigative solutions to Insurance, Government, Self-Insured, and Third Party Claims Administrators.

What is SmartPartner?

Developed by CoventBridge, SmartPartner is the industry leading case management platform. It is an industry leading platform that features a secure, user friendly web application to comprehensively administer and manage the complete lifecycle of all investigate efforts and activities. The system is completely custom and proprietary, written entirely in-house by full-time application developers, in tandem with Sales and Operations personnel, to achieve an efficient, agile platform to service the needs of our clients.

SmartPartner is comprised of several portals or modules that provide role-based access by specific functionality. These portals have evolved over time to meet the demands of both growing company requirements and specific customer requests. The SmartPartner application is continually enhanced to improve efficiencies for our customers and our employees.

Information in SmartPartner

SmartPartner contains Personally Identifiable Information (PII), Protected Health Information (PHI), and non-sensitive information to support insurance fraud investigations. Depending on the SmartPartner portal, information can include name, medical information, and employment information to referral data and invoices.

The stored information is maintained within the SmartPartner database, which is secured, encrypted (AES-256), and compliant with HIPAA security requirements and SOC 2 Type 2 standards.

Information Security

Information Security Management

In support of a holistic and structured approach to managing information security, CoventBridge's management adheres to the NIST Cybersecurity Framework. This provides the framework for the policies and procedures our management team has adopted to implement into information systems. This implementation is based on the NIST Risk Management Framework (RMF) standard and incorporates controls from the Trust Services Principles and Criteria for Security and Availability, as required to maintain our SOC 2 Type 2 audit report.

Governance Risk and Compliance

Executive Oversight

Senior management is a key IT stakeholder. They provide executive oversight over information systems including strategic direction, leadership, and resource support to the IT Infrastructure & Operations, App Development, and Information Security departments.

To achieve an effective and disciplined governance program over these departments, senior management adheres to an IT Strategic Plan to identify goals, objectives, and measurable benchmarks. The plan provides a roadmap to address both the current state and technological and operational ambitions.

Risk Management Framework

CoventBridge implements the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF), which integrates security and risk management activities into the system development life cycle (SDLC).

GDPR

CoventBridge complies with the General Data Protection Regulation (GDPR) to ensure data and privacy are protected for all individuals within the European Union (EU), as well as the exportation of personal data outside the EU. In addition, CoventBridge adheres to the six privacy principles of GDPR:

- Lawfulness, Fairness, and Transparency
- Limitations on Purposes of Collection, Processing, and Storage
- Data Minimization
- Accuracy of Data
- Data Storage Limits
- Integrity and Confidentiality

Below are several of our GDPR initiatives:

- We implement technical controls, such as the secure storage of encryption keys, for personal data.
- We ensure that all employees with access to customers' personal data have been trained in handling that data and are bound to maintain the confidentiality and security of that data.
- We hold any vendors that handle personal data to the same security and privacy practices and standards to which we hold ourselves.

CCPA

CoventBridge complies with the California Consumer Privacy Act (CCPA), which regulates how businesses are allowed to handle the personal information of California residents. CCPA contains clear and precise compliance requirements that CoventBridge meets by:

- Updating our privacy policy with information on how, why, and what personal information we collect and process.
- Updating our privacy policy with information on how users can request access, change, or erasure of their personal data that has been collected.

Privacy Program

CoventBridge has a published privacy policy that clearly defines what data is collected and how it is used. We understand that the privacy of information entrusted to us is paramount, and we're committed to customer privacy and transparency.

CoventBridge takes steps to protect the privacy of our customers and protect data stored within the platform. Some of the protections inherent to our products include authentication, access controls, data transport encryption, HTTPS support for customer applications, and the ability for customers to encrypt stored data. In addition, we implement the following NIST privacy controls:

- Authority and Purpose (AP)
- Accountability, Audit, and Risk Management (AR)
- Data Quality and Integrity (DI)
- Data Minimization and Retention (DM)
- Individual Participation Redress (IP)
- Security (SE)
- Transparency (TR)
- Use limitation (UL)

Corporate and Operation Security

Identity and Access Management

CoventBridge defines and manages the roles and access privileges of individual network users and the way in which users are granted privileges. Whether it's an employee or customer, identity and access management is necessary so there is one digital identity per individual. This is modified, monitored, and maintained throughout the identity and access management lifecycle.

Principles of Least Privilege

The principle of least privilege applies to all users (privileged and standard), programs, and processes. The bare minimum access necessary to perform a function is given. The periodic access reviews, as mentioned above, are one approach to ensure the principle of least privilege is properly enforced.

Segregation of Duties

CoventBridge has created a segregation of duties (SoD) matrix to help reduce the potential damage that could be caused from the actions of one individual. The SoD is enforced when assigning roles to new or existing users.

Privileged Access Management

Across the environment, there are controls in place to manage, secure, control, and monitor privileged access and permissions for users, processes, accounts, and systems. The Privileged Access Management system is centralized, making it easier to manage privileged credentials in one place.

Multifactor Authentication

Multifactor Authentication (MFA) is required to access the network and information system resources. With MFA in place, this creates multiple layers of security to help increase confidence that the user requesting access is who they say they are.

Access Reviews

CoventBridge requires that system access reviews be performed on a quarterly basis to ensure administrative access to production systems is limited and based on appropriate roles and responsibilities. Automated scheduled audit logs are sent to the security team to ensure a comprehensive access review is completed in a timely manner.

Awareness and Training

General Awareness

Everyone at CoventBridge receives security and privacy awareness training, both as part of their onboarding and as an ongoing refresher. At CoventBridge, every employee receives training to promote security awareness and company culture covering the following topics:

- General Information Security Overview
- Phishing Awareness and Prevention
- Office Physical Security and Clean Desk Policy
- Password Policy and Management
- Security Incident Management
- Privacy and Data Protection

Training is followed up with periodic phishing exercises and clean desk checks.

Roles-Based Training

To ensure all CoventBridge developers have a consistent level of application security, knowledge training is mandatory for all current and new developer hires. Developers must complete the role-based training upon hire along with several electives.

Configuration Management

CoventBridge has a formal Change Management Policy and Procedures in place, which communicate management's expectations regarding the change process to employees to ensure unauthorized changes are not made to production systems. These policies and procedures address the production infrastructure and software development lifecycle including change requests, approvals, and standard change implementation procedures to guide employees through the implementation of commonly applied changes.

Security Operations**24x7 SOC Capabilities**

CoventBridge has a 24/7 Security Operations Center (SOC) to handle any malicious and damaging activity that could happen at any hour. The SOC team is responsible for detecting and responding to security threats.

Endpoint Protection (Detection, Response, and Protection)

An endpoint protection solution has been deployed to protect endpoints such as servers and workstations that are used to connect to the CoventBridge network. Our endpoint solution delivers antivirus, anti-spyware, and other types of intrusion prevention capabilities. The endpoint solution is used by the SOC team for incident response and detection.

Vulnerability and Patch Management

To better manage network security, CoventBridge regularly checks for vulnerabilities with firewall logging, network scanning, and penetration testing. After an analysis, if there are any vulnerabilities detected, we perform patches or other tactics for remediation in a timely manner.

Periodic Security Control Assessments

Periodic Security Control Assessments are performed annually to stay in compliance with NIST 800-53 control requirements. The Information System owner's dependent on common controls that are less than effective consider whether they are willing to accept the associated risk or if additional tailoring is required to address the weaknesses or deficiencies in the controls.

Security Incident Management**Incident Response Plan and Handling Capabilities**

CoventBridge has an incident response team that follows the incident response plan and handling capabilities put in place to better detect, respond, and recover from network security events. This plan addresses data loss, cybercrime, and outages that threaten business objectives.

Incident Response Training, Tests and Exercises

CoventBridge requires key personnel to undergo incident response training, as well as tabletop exercises. This ensures the incident response team and key personnel have a clear understanding of the incident response plan and handling capabilities.

Business Continuity

Redundancy

In the event of an outage or any other system disruption, redundancy is put into place to allow the business to continue as usual. This includes redundant firewall interfaces, redundant hand-off switches, redundant network hand-offs for major facility hubs of operations, and geographically redundant storage servers.

Availability

CoventBridge has geographically diverse sites, which ensures a high level of availability in the event of an outage in a specific geographic region. Our multiple levels of hardware redundancy allow users to continue performing business as usual.

Backups

CoventBridge performs disk-based backups and uses additional cloud storage. We implement best practices for storing backups and encrypt any data prior to transport for backups stored offsite.

SmartPartner Application Security

Infrastructure

SmartPartner is built on a scalable infrastructure. It is hosted and managed on Amazon Web Services (AWS) across multiple zones to support fault tolerance, high availability, and disaster recovery.

Software Development Lifecycle

SmartPartner follows the CoventBridge IT Project Methodology. There are 7 phases within the methodology, each with varying deliverables and artifacts, with a continual focus on project integrity and quality through all phases.

Encryption

We encrypt SmartPartner data both in transit and at rest. Data is protected in transit using SSL (HTTPS) or Secure FTP (SFTP) and stored encrypted at rest (AES-256).

Key Management

CoventBridge uses the AWS Key Management Service (KMS) for encryption key management. AWS KMS is designed so that no one, including AWS employees, can retrieve master keys from KMS and decrypt SmartPartner data. AWS KMS is regularly audited and certified under an encryption standard (FIPS 140-2) such that an independent third party has verified it meets the highest level of cryptographic standards.

Authentication

SmartPartner provides authentication services that leverage the existing Microsoft Active Directory authentication.

To prevent unauthorized account access to SmartPartner, we enforce the following:

- Strong passphrase for user account and encryption keys
- Secure storage of encryption keys to prevent disclosure
- Replacement of encryption keys if lost or disclosed
- Role-Based Access Control (RBAC) model

Role-Based Access

SmartPartner is built with robust groups and permissions system, which enables privileged users to restrict which content certain users can view or edit. With this approach, role-based access control gives employees access to only the information necessary to perform their jobs.

Product Security Testing

CoventBridge performs security testing internally and externally. Dynamic application security testing is performed to detect security vulnerabilities such as cross-site scripting (XSS) and SQL injection. External penetration testing is performed on an annual basis to detect any malicious code and other potential vulnerabilities. Those specific vulnerabilities that can be found within the OWASP top 10 are identified as high risk.

Application Security Testing

CoventBridge performs Application Security Testing to help an organization determine whether SmartPartner contains vulnerabilities that can be exploited, and whether the software behaves and interacts securely with its users, other applications (such as databases), and its execution environment.

OWASP Top 10

The SmartPartner developers proactively update and maintain the platform while keeping the OWASP Top 10 in mind. The OWASP Top 10 is a standard awareness document for developers and web application security. A full list and its descriptions can be found here: <https://owasp.org/www-project-top-ten/>.

Below are the Top 10 Web Application Security Risks as of 2020:

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities.
10. Insufficient Logging & Monitoring

Appendices

Please note that the files in the appendix are only available when opening the PDF in Adobe Reader. Attachments will not be accessible when opening this PDF in a browser such as Chrome.

1. SOC 2 Type 2 Report
2. Corporate Security Policy
3. Vendor and Affiliates Policy
4. Trusted Vendors