VSA CORE Questionnaire 2019 FINAL

What is the CORE Questionnaire?

The VSA CORE questionnaire focuses on security and privacy principles and practices. From a security viewpoint, it does not go into the same depth as the full VSA FULL questionnaire but hits the key points. It also adds the Privacy section(s), required by companies based in the USA and worldwide

The VSA CORE questionnaire should be used when companies wish to ensure the vendor has well designed security & privacy operations. The VSA FULL focuses on security only, and goes into more depth than the VSA Core

Why Audit Vendors?

When we do business with a vendor, it is not safe to assume we are doing business just with the party under contract. Vendors rely on other parties. If we are to rely on a chain, then all the links must be tested, not just the first link. We must also apply the same standard of testing to all the links, which is why we created this questionnaire.

Approaches Taken

1) Data-Risk Based: Not all vendors should be held to the same standard. The risk is proprtionate to the sensitivity of the data they are accessing (and the volume of data). The controls vendors should have in place must be proprtionate to their risk.

2) Integrated Security: Great security is not achieved by purchasing a product. It is achieved by thinking about security from the start; how a product is designed, how a product is tested, how it is patched and maintained, what steps have been taken to minimise a breach and what happens during a security incident. All of these and more are covered in this questionnaire.

3) Service oriented. Many companies have multiple offerings of services and products. Rather than audit the company, we focus on just the services that are being delivered. Only the security policies and controls in the scope of the service under review are relevant. Vendors should fill the questionnaire out for each specific product or package that is being evaluated.

Automated Scoring?

There are those who strive to automate scoring. In our experience this has a negative correlation with true security status. As a result, we ask many open questions. The nuances of the answers reveal both good and bad security practices and philosophies, something automated scoring cannot.

The Privacy sections are far more compatible with automated scoring than the Security section

How should a non-VSA member use this questionnaire?

a) Send this questionnaire to your vendors to assess their cybersecurity risk. They will return it directly to you, and you can assess their risk, and

b) Use this questionnaire to benchmark the cybersecurity risk of services you provide, and find areas to improve

How should a VSA member use this questionnaire?

(i) You have the same options as non-VSA members, or

(ii) You can leverage VSA to have independent third party auditors carry out your third party audits. This will greatly shorten the time and cost to vendor approval or rejection decisions.

How can I become a VSA member?

Email us at membership@vendorsecurityalliance.org

What is the VSA?

The VSA is a coalition of companies focused on measuring and reducing vendor risk, with the goal of making the internet safer for everyone. The VSA is a non-profit entity.

FAQs

Scope: If a question is ambiguous regarding scope, answer it within the scope of delivery of the service under audit.

What is the definition of 'X': Please see the final tab in this document

Special thanks to the Working Group that created this document:

Ken Baylor https://www.linkedin.com/in/kenbaylor
Gary Miller https://www.linkedin.com/in/gary-miller-56a2111/
Karim Adib https://www.linkedin.com/in/karim-adib-24120b8b/
Jan Encina https://www.linkedin.com/in/jan-martin-encina-0b4b8445/
Jack Baylor https://www.linkedin.com/in/jackbaylor/

			Vendor Response			Description/Link
			Yes	No	N/A	
1	**Business Information**					
	a	Company name				strongDM, Inc.
	b	Responder Name				Craine Runton
	c	Responder Contact Information (Phone/Business Email Address)				security@strongdm.com
	d	Date of Response				April, 2021
2	**Company Profile**					
	a	Company Website URL				https://www.strongdm.com
	b	Service Website URL				https://app.strongdm.com
3	**Service Scope Question**					
	a	Name of application or service being provided				strongDM Platform
	b	Description of application or service				strongDM offers data and infrastructure security software that is utilized by technology teams to increase the security, transparency, and convenience of accessing secure systems. The strongDM SaaS System is a proxy that manages and audits access to databases, servers, clusters, and web apps. It is comprised of a local client, gateway intermediary, and configuration layer. The strongDM SaaS System is delivered as a Business-to-Business SaaS product.
	c	What technology languages/platforms/stacks/components are utilized in the scope of the application? (AWS? MySQL? Ruby on Rails? Go? Javascript?)				strongDM relies on a number of technology stacks and is primarily deployed in Amazon Web Services. Within AWS we rely on the following services: EC2 RDS KMS ELB S3 Route53 Our gateway/relay application is written in Golang prior to compilation into distributed binaries. Our web applications rely on a number of JavaScript frameworks.

4	**Service Hosting**					
	a	Is your service run from your own (a) data center, (b) the cloud, or (c) deployed-on premise only				The strongDM Platform runs exclusively in the cloud
	b	Which cloud providers do you rely on?				Amazon Web Services
	c	Have you researched your cloud providers best security practices?				Yes
	d	Which data centers/countries/geographies are you deployed in?				US-East-2
	e	On-premise solution only				N/A
	f	Hybrid Solution (on-premise, cloud): Please explain				N/A
5	**Supporting Documentation**					
		Please attach the following documents for review (if existing):				
	a	Most recent Application Code Review or Penetration Testing Reports (carried out by independent third party). If an independednt third party report is not available, please enter 'Not Completed'				An executive summary of our most recent penetration test is provided upon request to customers and prospects under MNDA
		Which industry approved methodology does the penetration test follow?				Our independent testing agency conducts gray-box testing of our web application and API.
	b	Information Security Policies and Procedures				Details of our information security policies and procedures are provided upon request to customers and prospects under MNDA
	c	Data Flow Diagram				Data flow diagrams are provided upon request to customers and prospects under MNDA
	d	Any other Documents supporting your responses in this questionnaire (Please provide a description for each document).				N/A
	e	PCI, SOC2 type II or ISO27001 certification reports				Our most recent SOC 2 Type 2 report is provided upon request to customers and prospects under MNDA
	f	Other Independent Audit report (please provide details)				N/A

			Vendor Response Yes	No	N/A	Description/Link
Data Protection & Access Controls						
	Data Classification					
1		Please describe the customer data you require to provide your service: personal information, financial data, confidential/sensitive data, government data				There are two components to the strongDM Platform that collect potentially sensitive customer information. The first is the collection of personal information about users to create user accounts. The information collected is First Name, Last Name, and Email Address. The second component is configuration of data sources within the Platform. The information collected here includes Datasource Name, IP Address or Hostname, and Authentication Data.
2		Please upload your data classification matrix including data definition, access restrictions and minimum controls specific for your service				A copy of our data classification matrix is provided upon request to customers and prospects under MNDA
	Encryption					
3		How do you encrypt customer data? Please upload relevant documentation				Customer data is encrypted at rest using standard configurations available within the AWS management console for instances created within RDS.
	Data Access & Handling					
4		Which groups of staff (individual contractors and full-time) have access to customer personal and sensitive data?				A limited number of production operations engineers and the Customer Engineering (Support) team have access to the database and customer information
5		Describe how offsite backups occur and how they are secured				strongDM configures regular point-in-time backups of its production database through the AWS management console. Only a limited number of production operations engineers are able to recall backups and perform a restore of the database.

	Authentication					
		Internal Use				
6		How are passwords hashed?				Passwords for strongDM Platform users who are not bound to an external SSO are hashed using bcrypt and current best practices for salting and iterations.
7		Is MFA required for employees/contractors to log in to production systems?	X			
Policies & Standards						
	Management Program					
8		Do you have a dedicated information security team? If so, what is the composition and reporting structure?	X			strongDM employs a Director, Security & Compliance who is responsible for executing the Information Security Program. This role reports directly to the CEO.
9		Do you have a formal Information Security Program (InfoSec SP) in place?	X			
10		Please describe your Information security risk management program (InfoSec RMP)?				strongDM has built its Risk Management Program around the relevant NIST 800-series Special Publications. We conduct regular risk assessments and risk sessions with leadership.
	Policy Execution					
11		Please ensure your documented information security policy has been uploaded in section in 'Service Overview'			X	A copy of our Information Security Policy can be provided upon request to customers and prospects under MNDA
12		Do your information security and privacy policies align with industry standards (ISO-27001, NIST Cyber Security Framework, ISO-22307, CoBIT, etc.)?	X			Yes, our Information Security Program is based on and aligned with the NIST Cybersecurity Framework v1.1
13		Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	X			
	Confidentiality					
14		Are all personnel required to sign Confidentiality Agreements to protect customer information, as a condition of employment?	X			

	Acceptable Use					
15		Are all personnel required to sign an Acceptable Use Policy? Please attach	X			We require all personnel to sign an AUP at time of hire. A copy of the AUP can be provided upon request to customers and prospects under MNDA
Proactive Security						
	Network and Application Security Testing					
16		How do you test the security of your network and applications? Internal, third parties or both? If so, what is the cadence? Explain your methodology				We conduct both static code analysis of all code committed to our repositories and conduct annual penetration testing of our web application and API.
	Vulnerability Management/Patching					
		Network/Host Vulnerability Management				
17		Please summarise or attach your network vulnerability management processes and procedures (specifying who executes the procedures and the tools used)?				We have a comprehensive vulnerability management program that covers all categories of vulnerabilities within the strongDM environment. Newly discovered vulnerabilities are assessed for severity, availability of public exploit code, etc, in order to prioritize remediation.
		Application Vulnerability Management				
18		Please summarise or attach your application vulnerability management processes and procedures (specifying who executes the procedures and the tools used)?				We have a comprehensive vulnerability management program that covers all categories of vulnerabilities within the strongDM environment. Newly discovered vulnerabilities are assessed for severity, availability of public exploit code, etc, in order to prioritize remediation.
		Production Patching				
19		How do you regularly evaluate patches and updates for your infrastructure?				We have a comprehensive vulnerability management program that covers all categories of vulnerabilities within the strongDM environment. Newly discovered vulnerabilities are assessed for severity, availability of public exploit code, etc, in order to prioritize remediation.
20		How does the criticality of the patch (critical, high, medium, low) affect deployment guidelines?				Both criticality and availability of exploit code are used to determine how quickly a given patch is deployed into the production environment

	Endpoint Security - End User					
21		Are all endpoint laptops that connect directly to production networks centrally managed?	X			
22		Describe both standard employee issued device security configuration/features and required BYOD configurations. (Login Password, antimalware, Full Disk Encryption, Administrative Privileges, Firewall, Auto-lock, etc.)				All employees are issued devices that have full-disk encryption, anti-virus/anti-malware, auto lock/screen timeouts, and minimum password length requirements. Each machine is centrally managed and policies are set by the organization. Employees are not permitted to use personal or BYOD systems to access the strongDM production environment or any customer data.
	Endpoint Security - Production Server					
23		What systems do you have in place that mitigate classes of web application vulnerabilities? (e.g.: WAF, proxies, etc)				We do not currently employ any technologies like web application firewalls on web ingress.
24		Do you have operational breach detection sytems, deception solutions and/or anomaly detection with alerting?				We employ a variety of solutions on our production servers to detect anomalous behavior and breaches
	Infrastructure Security					
		Secrets Management				
25		Describe your secrets management strategy:(auth tokens, passwords, API credentials, certificates)				Secrets that are part of our Platform are stored either in Amazon's Key Management System. For customers, authentication secrets are stored in a customer's secret store such as HashiCorp Vault or AWS Secrets Manager.
		Logs				
26		Are all security events (authentication events, SSH session commands, privilege elevations) in production logged?	X			
		Network Security				
27		Is the production network segmented in to different zones based on security levels?	X			
28		What is the process for making changes to the network configuration?				All network configurations are source-controlled through Terraform, and all changes to the Terraform configuration are reviewed by at least 2 engineers prior to being implemented, and must be implemented by a third production operator.

	Cryptography					
		Cryptographic Design				
29		What cryptographic frameworks are used to secure a) data in transit over public networks, b) passwords, c) data at rest?				We use TLSv1.2 to encrypt all connections made over public networks. Passwords are hashed using bcrypt with current recommendations for salting and rounds. The framework depends on the service that is encrypting the data at rest, but we do employ encryption at rest on all our production systems.
		Key Management				
30		How are crytographic keys(key management system, etc) managed within your system?				We delegate management of cryptographic keys to AWS KMS.
	Security Awareness					
31		Describe your security awareness program for personnel				All employees are required to attend a yearly security awareness training, and the Director, Security & Compliance regularly updates the company on evolving threats.
Reactive Security						
	Monitoring					
32		How do you log and alert on relevant security events? (this includes the network and application layer)?				We log and alert on security events related to the service provided using a variety of tools, and engineers respond to those alerts with investigation and remediation if necessary.
	Incident Response					
33		Describe or attach your Security Incident Response Program?				Our Incident Response Program is based on the Incident Command System. Roles are clearly defined and the procedures are tested on a quarterly basis.
	Incident Communication					
34		Do you have formally defined criteria for notifying a client during an incident that might impact the security of their data or systems? What are your SLAs for notification?		X		

Software Supply Chain						
	Secure SDLC					
35		How do you ensure code is being developed securely?				We maintain custom static analysis and linting code. Every developer contributes to that system and responds to security alerts. Each commit is authored and reviewed by a pair of developers with responsibilities for cross-training for secure coding practices as part of the code review process.
36		How do you train developers in SSDLC / Secure Coding Practices?				We maintain custom static analysis and linting code. Every developer contributes to that system and responds to security alerts. Each commit is authored and reviewed by a pair of developers with responsibilities for cross-training for secure coding practices as part of the code review process.
Customer Facing Application Security						
	Authentication					
37		Please describe how you authenticate users: If passwords are used, describe complexity requirements, and how passwords are protected. If SSO is supported, please describe the available options. If different service tiers are available, please describe.				Customers can select either a native logon or an SSO option. Native authentication allows a customer administrator to specify the password complexity requirements enforced on that customer's users. SSO authentication is available with the following providers (as of 04/2021): ADFS Auth0 Azure Google Keycloak Okta OneLogin v2 VMware

	Role Based Access Control					
38		Does your application enable custom granular permissions and roles to be created? Please describe the roles available				Yes. The strongDM Platform has two distinct sets of roles within it. The first set of roles consist of the application roles as defined by strongDM, as they relate to the Platform. **Account Administrator** - Has full access to the entire organization **Database Administrator** - Has access to create and configure datasources and servers **Team Leader** - Has access to manage users within a particular role **User** - Has access to datasources and servers to which they have been granted The second set of roles are defined by a customer, and grant access to a group of data sources to the users within that group.
	Audit logging					
39		Which audit trails and logs are kept for systems and applications with access to customer data?				All access to production systems (and the customer data resident in them) is strictly controlled through the strongDM Platform, providing a full audit trail of all actions taken on those systems.
	API Management					
40		How does your application store API keys?				Secrets that are part of our Platform are stored in Amazon's Key Management System.
Compliance						
	Internal Audits					
41		How do you conduct internal audits (audits lead by your personnel) of the service? please describe the scope, remediation process and frequency of audits.		**X**		
	External Audits					
42		How do you conduct external (third-party) audits of the service? please describe the scope and frequency of audits.				Yes. We conduct an independent SOC 2 Type 2 audit annually which covers the security, confidentiality, and availability of the strongDM Platform.
a		Please provide a copy of the most recent report (as per Service Introduction tab, section 5).				Our most recent SOC 2 Type 2 report is provided upon request to customers and prospects under MNDA

	Certifications					
43		Which IT operational, security, privacy related standards, certifications and/or regulations you do comply with?				We base our Information Security Program on the NIST Cybersecurity Framework v1.1, and have a SOC 2 attestation.
a		Please provide a copy of the most recent report (as per Service Introduction tab, section 5).			X	Our most recent SOC 2 Type 2 report is provided upon request to customers and prospects under MNDA
	Privacy					
44		Do you seek a right to use or own customer derived data for your own purposes? Please describe		X		
45		Is your Privacy Notice/ Privacy Policy externally available? Please provide the URL.	X			https://www.strongdm.com/privacy

In this section there are 2 options: USA or GDPR

Companies may select the one that is most appropriate for them, or both, or neither. Customers who have data subjects/consumers in USA will generally insist vendors complete the USA section, while those from the EEA/Philippines will insist vendors complete the GDPR section

USA Privacy

This area covers questions relating to the core principles of USA data breach laws, and the California Consumer Protection Act (CCPA). Out of scope are business that involve the personal information of those under the age of 16

GDPR

This area covers questions relating to the core principles of the General Data Protection Regulation which came into effect in May 2018. The questions are based on the standard contractual clauses and the extra requirements needed by GDPR.

For the purposes of this questionnaire the terms 'data subject' and 'consumer' shall be equivalent

			Vendor Response			Description/Link
			Yes	No	N/A	
State Notification Laws						
1		In the event of a data breach (involving a consumers name together with either that person's 1) SSN 2) Drivers license number, 3) financial account information together with the means of accessing their funds 4) Passport numbers or 5) Medical/Health/Biometric information), do you warrant you will disclose this event immediately (unless delayed for criminal investigation purposes)?			X	strongDM does not collect personal information beyond first name, last name, and work email address
	CCPA					
2	1798.100.	Prior to collection of personal information, do you inform consumers as to the categories of personal information to be collected and the purposes for which this will be used?			X	strongDM does not collect personal information from consumers
3		Do you have a mechanism to provide a copy of the collected consumer personal information, free of charge, to the consumer with 45 calendar days of receiving the request? Please link to or describe the mechanism		X		
4	1798.105.	Do you have a mechanism to delete your collected consumer personal information, free of charge, upon receiving a verified consumer deletion request? Please link to or describe the mechanism		X		
5		Is this deletion request cascaded to your service providers?			X	
6	1798.110.	Are the following available on your public website: (1) The categories of personal information you collect about consumers. (2) The categories of sources from which the personal information is collected. (3) The business or commercial purpose for collecting or selling personal information. (4) The categories of third parties with whom the business shares personal information. (5) Description of procedure the consumer may follow to obtain a copy of the specific pieces of personal information the you have collected about that consumer. The list of categories of personal information a) disclosed for a business purpose, and b) sold, should be separate lists under 1798.130.(5)(c) Please provide the appropriate URL		X		strongDM does not collect personal information from consumers

7	1798.115.	If your company sells consumer personal information, or discloses it for a business purpose, please describe the mechanism to disclose to the consumer: (1) The categories of personal information that the business collected about the consumer. (2) The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold. (3) The categories of personal information that the business disclosed about the consumer for a business purpose The list of categories of personal information a) disclosed for a business purpose, and b) sold, should be separate lists under 1798.130.(5)(c) Please provide the appropriate URL			X	strongDM does not sell any consumer information
8		If you resell personal information obatained other than directly from your consumers: do you refrain from selling personal information about a consumer unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out?			X	strongDM does not sell any consumer information
9	1798.120.	If your business sells personal information to third parties, how do you inform customers a) that you sell their information b) of their right to opt-out of having their personal information sold c) How do consumers execute their ability to opt-out			X	strongDM does not sell any personal information
10	1798.125.	Do you assure the same level of service to consumers who have exercised their rights under CCPA?			X	strongDM does not collect personal information from consumers
11	1798.130.	Do you provide a minimum of two methods to contact you to submit consumer requests for information (e.g. website address, toll free number)? Please link to or describe the mechanism			X	
12		Do you have a publicly available notice on your website and/or App describing CCPA rights, and how requests should be submitted? Please link to it		X		
13	1798.135.	Do you have a clear and conspicuous link on your homepage titled: "Do Not Sell My Personal Information" which enables a consumer to opt out of the sale of personal information (without having to create an account just for that purpose)? Or do you implement a different mechanism to enact the same rights for California consumers?		X		
	Training					
14		Are the people handling personal information trained in their privacy obligations, at least annually?		X		

		Vendor Response			Description/Link
		Yes	No	N/A	
	GDPR PROCESSING				
	Fundamentals: Do you agree to the following terms when processing data on behalf of your customer				
1	The data received by the Processor remains the property of the Controller at all times unless ownership is explicitly shared or transferred by a written agreement	X			
2	The Processor will follow and not derivate from the processing instructions of the controller. If unable to do so (for technical or GDPR compliance reasons) the Processor will promptly inform the Controller		X		
3	The Processor must not use sub Processors without advanced notification or consent of the Controller;		X		
4	All sub Processors must have equivalent security and privacy controls to those of Processor.	X			
5	The Processor shall cooperate with the relevant Data Protection Authorities in the event of an enquiry;	X			
6	The Processor must keep all received information confidential;	X			
7	The Processor must report data breaches to the Controller without delay. In all cases within 72 hours of becoming aware of the breach.		X		strongDM does not currently publish an SLA for notifying customers of a data breach involving their data beyond that we will inform customers in a timely manner
8	The Processor must assist the Data Controller in managing the consequences of data breaches to the GDPR standard			X	
9	The Processor shall keep records of all processing activities		X		
10	The Processor is willing to assist the Controller to comply with data subjects rights requests	X			
11	The Processor must delete or return all personal data at the end of the contract, at the choice of the Controller	X			Upon written request from a departing customer, strongDM will delete and/or anonymize all personal and other data from our systems
12	The Processor implements adequate measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access	X			
13	If based in the USA, are you currently a member of Privacy Shield?		X		
14	Are your DPO contact details displayed prominently on your website privacy notice?		X		

	GDPR Addenda: Do you agree to the following terms when processing data on behalf of your customer				
15	Data will only be processed as long as it is needed for business and legal reasons as envisioned when the data was submitted by the relevant parties	X			
16	All parties (including sub contractors) authorized to process the personal data covered by this contract are committed to protect the confidentiality of the data			X	
17	In the event of a request by a data subject, the processor will reasonably assist the controller to respond to the data subject in an accurate and timely manner.			X	
18	Service provider will cooperate with controller in the event the controller initiates a data protection impact assessment			X	
19	The processor is not permitted to engage in onward transfers to additional countries outside of the EEA, without the explicit permission of the customer, in advance.			X	
20	Are the people handling personal information trained in their privacy obligations, at least annually?		X		

Bug bounty program: any method by which members of the public can submit to a company information regarding security vulnerabilities, software to fix an issue, or any other deviation of the company's software that does not fit its intended purpose.

Confidential/Sensitive data: any information a reasonable person would consider private, or not choose to share publicly. It can also include: (a) Information about criminal convictions and offences, (b) data revealing: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, (c) genetic data, biometric data, data concerning health or data concerning a person's sex life or sexual orientation or (d) financial data, drivers license number, social security numbers.

Critical Security Vulnerability: a vulnerability is a state in a computing system (or set of systems) that either:
1) allows an attacker to execute commands as another user, or
2) allows an attacker to access data that is contrary to the specified access restrictions for that data, or
3) allows an attacker to pose as another entity, or
4) allows an attacker to conduct a denial of service

Customer Data: Data your application or service recieves from a customer

Data Classification Policy (or Matrix): A policy or matrix classifying data by risk and applying appropriate controls to safeguard the data.

Data Encryption Standard: A document describing the security method (including Algorithms) used to encryption information, e.g. AES-256

Data Flow Diagram: A diagram showing how data flow through the infrastructure and applications, from ingestion onwards.

Financial Data: Data such as credit card numbers, credit ratings, account balances, and other monetary facts about a person or organization that are used in billing, credit assessment, loan transactions, and other financial activities.

Individual contractors: any non-employee that works under the direct control of the employer.

Multifactor authentication (MFA): a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction

Partner: any person or business entity with an agreement to share work with the company

Penetration Test approved methodology: a penetration test that follows one of the frameworks listed here:

- Open Source Security Testing Methodology Manual (“OSSTMM”)
- The National Institute of Standards and Technology (“NIST”) Special Publication 800-115
- OWASP Testing Guide
- PCI Penetration Testing Guidance
- Penetration Testing Execution Standard
- Penetration Testing Framework

Penetration Test: the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit. Every vulnerability discovered is disclosed to the customer.

Personally Identifiable Information (PII): any information, on its own or when combined with other information, that can be individually attributed to identify an individual. This information includes, but is not limited to, drivers license numbers, social security numbers (or their equivalent), health and financial records.,

Personnel: Includes employees and contractors under the direct control of management.

Privacy Incident: A privacy incident results from the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, alteration or any similar term referring to situations where persons other than authorized users, and for an other than authorized purpose, have access or potential access to PII in usable form, whether physical or electronic. The term encompasses both suspected and confirmed incidents involving PII that raise a reasonable risk of harm

Protected Data: Includes PII, sensitive data, HIPAA, financial data and other data defined as sensitive data

Role-based Access Control: A methodology to assign and manage appropriate level of access control to all computer systems in an organization or enterprise based on job functions and responsibilities.

Security Incident: An incident is any event that threatens the security, confidentiality, integrity, or availability of information assets (electronic or paper), information systems, and/or the networks that deliver the information. An incident can involve:

1) violation of an explicit or implied security policy
2) attempts to gain unauthorized access
3) unwanted denial of resources
4) unauthorized use
5) changes without the owner's knowledge, instruction, or consent

Vendor Audit: A process in which a vendors security controls are validated by an approved method. The deliverable is access to the audited report(s) of the vendor service, which involves either triggering a new audit or gaining access to a current audit report for the vendor.

Web application firewall (WAF): A web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked. The effort to perform this customization can be significant and needs to be maintained as the application is modified.

EU Specific terms from General Data Protection Regulation

Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Data Protection Officer (DPO): Role defined by articles 37-39 GDPR

Data Subject: An identified or identifiable natural person

Personal Data or Personal Information: any information relating to an identified or identifiable natural person ('data subject');

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Recipient: a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

Third Party: a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data;

Disclaimer and Limited License Grant. The Vendor Security Alliance (VSA) questionnaire and all related material (the "Licensed Material") is provided AS IS, with no representations or warranties of any kind, whether express, implied, statutory, or other. This includes, without limitation, warranties of title, merchantability, fitness for a particular purpose, non-infringement, absence of latent or other defects, accuracy, or the absence of errors, whether or not known or discoverable. VSA and its members will have no liability under any legal theory (including, without limitation, negligence) or otherwise for any direct, special, indirect, incidental, consequential, punitive, exemplary, or other losses, costs, expenses, or damages arising out of use of the Licensed Material, even if advised of the possibility of such losses, costs, expenses, or damages.

VSA grants a limited right, under its copyright rights in the Licensed Material, for users of the Licensed Material to download a copy of the Licensed Material and reproduce and distribute unmodified copies for sole purpose of (a) a particular user evaluating its own internal security processes and the security practices of its direct vendors, or (b) providing Feedback to VSA. All other uses are prohibited (including, without limitation, using the Licensed Material in connection with a security consulting or hosted vendor management service), and no additional intellectual property rights are granted by VSA to any party. "Feedback" means any suggested changes to the Licensed Material. VSA will have the right to reproduce, distribute, perform, display and create derivative works of all Feedback, and use all Feedback without restriction and without payments to any party.