EXHIBIT D

DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY
AND
SUPPLEMENTAL INFORMATION ABOUT THE MLSA

1. **Purpose**

(a) This Exhibit supplements the Master License and Service Agreement ("MLSA") to which it is attached, to ensure that the MLSA conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of Erie 1 BOCES' Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the MLSA that is required to be posted on Erie 1 BOCES' website.

(b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that Vendor has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the MLSA, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. **Definitions**

Any capitalized term used within this Exhibit that is also found in the MLSA will have the same definition as contained within the MLSA.

In addition, as used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor's Product.

(d) "Participating Educational Agency" means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with a BOCES, and as a result is licensed to use Vendor's Product pursuant to the terms of the MLSA. For purposes of this Exhibit, the term also includes Erie 1 BOCES or another BOCES that is licensed to use Vendor's Product pursuant to the MLSA to support its own educational programs or operations.

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and Erie 1 BOCES's policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy. Erie 1 BOCES will provide Vendor with a copy of its policy and Vendor and Erie 1 BOCES agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure Vendor's continued compliance with Section 2-d.

4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with Erie 1 BOCES' Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.

Additional elements of Vendor's Data Security and Privacy Plan are as follows:

(a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.

(b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the MLSA: See Attachment 1.

(c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the MLSA" below.

(d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.

(e) Vendor [*check one*] _____will __☒___will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.

(g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

5. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the MLSA and the terms of this Data Sharing and Confidentiality Agreement:

(a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the MLSA.

(c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the MLSA, unless:

(i) the parent or eligible student has provided prior written consent; or

(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Promptly reimburse Erie 1 BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. **Notification of Breach and Unauthorized Release**

(a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b) Vendor will provide such notification to Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).

(c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the

incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.

(e) Vendor will consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

EXHIBIT D (CONTINUED)

ERIE 1 BOCES

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the community of the following:

(1) A student's personally identifiable information cannot be sold or released for any commercial purposes.

(2) Parents have the right to inspect and review the complete contents of their child's education record.

(3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

(4) A complete list of all student data elements collected by the State is available for public review at **http://www.nysed.gov/data-privacy-security/student-data-inventory**, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website **http://www.nysed.gov/data-privacy-security/report-improper-disclosure**.

BY THE VENDOR:

Eric S. Eder
Signature

Eric S. Eder
Printed Name

Founder
Title

February 12, 2021
Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND *CYBERFORCE|Q, LLC*

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") with *CyberForce|Q, LLC* which governs the availability to Participating Educational Agencies of the following Product(s):

Q|FRAME Cybersecurity Measurement Application

Pursuant to the MLSA, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law ("Protected Data").

Exclusive Purpose for which Protected Data will be Used: The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the MLSA. Protected Data received by Vendor, or any of Vendor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

Oversight of Subcontractors: In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by: We are not using subcontractors.

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on February 15, 2021 and expires on June 30, 2024.
- Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.

- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

				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	X			CyberForce|Q does not require any significant personal, financial, or government data to provide Q|FRAME services.
	2		Please upload your data classification matrix including data definition, access restrictions and minimum controls specific for your service	X			CyberForce|Q classifies sensitive data and has implemented access controls for each category of data.
		Encryption					
	3		How do you encrypt customer data? Please upload relevant documentation	X			Secrets are maintained with an encrypted and hardened configuration management system. Where appropriate, BitLocker is deployed.
		Data Access & Handling					
	4		Which groups of staff (individual contractors and full-time) have access to customer personal and sensitive data?	X			Only CyberForce|Q team members have access to sensitive CyberForce|Q data, and these team members are subjected to a variety of access controls - including
	5		Describe how offsite backups occur and how they are secured	X			Backups are only maintained within secure data centers utilizing layers of both physical and technical access controls. Connections between data centers are
		Authentication					
	6	**Internal Use**	How are passwords hashed?	X			CyberForce|Q passwords are hashed within Microsoft Active Directory.
	7		Is MFA required for employees/contractors to log in to production systems?	X			CyberForce|Q does require MFA to access production systems. Multi-factor authentication requires a registered mobile device (no e-mail or text MFA).
Policies & Standards							
		Management Program					
	8		Do you have a dedicated information security team? If so, what is the composition and reporting structure?	X			CyberForce|Q does have a dedicated information security team which is operational on a 24x7 basis. The team reports to a dedicated leader.
	9		Do you have a formal Information Security Program (InfoSec SP) in place?	X			CyberForce|Q does have a formal Information Security program, which is aligned to the NIST Cybersecurity Framework and various additional specialized control
	10		Please describe your Information security risk management program (InfoSec RMP)?	X			CyberForce|Q risk management program considers threats, vulnerabilities, likelihoods, and impacts to quantify and prioritize risks.
		Policy Execution					
	11		Please ensure your documented information security policy has been uploaded in section in 'Service Overview'	X			CyberForce|Q's information security policy aligns to the NIST Cybersecurity Framework along with additional specialized requirements.
	12		Do your information security and privacy policies align with industry standards (ISO-27001, NIST Cyber Security Framework, ISO-22307, CoBIT, etc.)?	X			CyberForce|Q's information security policy aligns to the NIST Cybersecurity Framework along with additional specialized requirements.
	13		Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures?	X			Yes, CyberForce|Q maintains a diciplinary policy.
		Confidentiality					
	14		Are all personnel required to sign Confidentiality Agreements to protect customer information, as a condition of employment?	X			Yes, CyberForce|Q personnel are required to sign Confidentiality Agreements.
		Acceptable Use					
	15		Are all personnel required to sign an Acceptable Use Policy? Please attach	X			Yes, CyberForce|Q personnel are required to sign Acceptable Use Policy.
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	X			CyberForce|Q relies primarily on internal cybersecurity expertise to perform security testing and validation. The cadence of security testing is
		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)?	X			CyberForce|Q performs network and host vulnerability management proactively. Identified vulnerabilities are directly remediated by experts within the
			Application Vulnerability Management				
	18		Please summarise or attach your application vulnerability management processes and procedures (specifying who executes the procedures and the tools used)?	X			CyberForce|Q performs application vulnerability management proactively. Identified vulnerabilities are directly remediated by experts within the
			Production Patching				
	19		How do you regularly evaluate patches and updates for your infrastructure?	X			CyberForce|Q evaluates patches on the basis of security impact and performance stablility. Critical patches are prioritized as time-sensitive and are addressed with
	20		guidelines?				
		Endpoint Security - End User					
	21		Are all endpoint laptops that connect directly to production networks centrally managed?	X			CyberForce|Q endpoint laptops are centrally managed. Non-managed devices are not authorized or able to access the production network.
	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.)	X			CyberForce|Q endpoints utilize hardened configurations. Disks are encrypted via BitLocker. "BYOD" or any other form of non-managed devices are not authorized or able to access CyberForce|Q resources.

				Vendor Response			
				Yes	No	N/A	Description/Link
		Endpoint Security - Production Server					
	23		What systems do you have in place that mitigate classes of web application vulnerabilities? (e.g.: WAF, proxies, etc)	X			CyberForce|Q maintains a web application firewall (WAF) which protects the Q|FRAME service.
	24		Do you have operational breach detection sytems, deception solutions and/or anomaly detection with alerting?	X			CyberForce|Q relies upon a wide variety of indicators and alerts to detect and assess events. The team monitors the Q|FRAME environment on a 24x7 basis.
		Infrastructure Security					
			Secrets Management				
	25		certificates)	X			management system.
			Logs				
	26		Are all security events (authentication events, SSH session commands, privilege elevations) in production logged?	X			CyberForce|Q security events are logged and triaged by staff.
			Network Security				
	27		Is the production network segmented in to different zones based on security levels?	X			highest zone of trust.
	28		What is the process for making changes to the network configuration?	X			CyberForce|Q network configuration changes must be documented and approved, prior to execution within dedicated change windows.
		Cryptography					
			Cryptographic Design				
	29		What cryptographic frameworks are used to secure a) data in transit over public networks, b) passwords, c) data at rest?	X			CyberForce|Q requires that all cryptographic mechanisms utilize widely-accepted, recommended ciphers such as AES256 and 3DES.
			Key Management				
	30		How are crytographic keys(key management system, etc) managed within your system?	X			Sensitive cryptographic keys are encrypted and subjected to specialized access controls via Microsoft Certificate Authority.
		Security Awareness					
	31		Describe your security awareness program for personnel	X			CyberForce|Q team members are required to pariticpate in organizational security awareness training. In addition, speciailized training for CyberForce|Q team
Reactive Security		**Monitoring**					
	32		How do you log and alert on relevant security events? (this includes the network and application layer)?	X			CyberForce|Q configures technology (both network and application technologies) to generate highly-detailed proacitve logging, logged to a SIEM.
		Incident Response					
	33		Describe or attach your Security Incident Response Program?	X			CyberForce|Q maintains procedures to proactively evaluate events. When incidents are identified, they are subjected to established runbooks and a nuanced
		Incident Communication					
	34		Do you have formally defined criteria for notifying a client durirg an incident that might impact the security of their data or systems? What are your SLAs for	X			CyberForce|Q establishes incident notification requirements with each client.
Software Supply Chain							
		Secure SDLC					
	35		How do you ensure code is being developed securely?	X			CyberForce|Q development is subjected to best-practices such as separate development and production environments, change control, secure coding
	36		How do you train developers in SSDLC / Secure Coding Practices?	X			CyberForce|Q development teams are required to train and adhere to security standards within their individual areas of specialization.
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	X			CyberForce|Q relies upon enhanced authentication. User passwords are subject to complexity enforcement, and multi-factor authentication is required for systems access. Multi-factor authentication requires a registered mobile device (no e-mail
		Role Based Access Control					
	38		Does your application enable custom granular permissions and roles to be created? Please describe the roles available	X			The Q|FRAME service does allow client participants to form specialized roles with customized privilege, including a "manager" role.
		Audit logging					
	39		customer data?	X			CyberForce|Q maintains the ability to audit access of any customer data.
		API Management					
	40		How does your application store API keys?	X			management system.

				Vendor Response			
				Yes	No	N/A	Description/Link
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			CyberForce|Q audits are conducted on a continuous basis and involve a combination of controls/technical assessment, impact analysis, and risk
		External Audits					
	42		How do you conduct external (third-party) audits of the service? please describe the scope and frequency of audits.		X		
	a		Please provide a copy of the most recent report (as per Service Introduction tab, section 5).				This assessment is being provided standalone - without any additional documentation, much of which is considered private/sensitive.
		Certifications					
	43		Which IT operational, security, privacy related standards, certifications and/or regulations you do comply with?		X		CyberForce|Q does not currently maintain formal certifications. However, the security program is aligned to a variety of standards and regulations such as NIST
	a		section 5).			X	N/A
		Privacy					
	44		Please describe		X		CyberForce|Q does not seek to use or own customer-derived data.
	45		Is your Privacy Notice/ Privacy Policy externally available? Please provide the URL.		X		CyberForce|Q does not host the privacy policy externally.

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

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

Critical Security Vulnerability: a vulnerability is a state in a computing system (or set of
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
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

Data Encryption Standard: A document describing the security method (including Algorithms)

Data Flow Diagram: A diagram showing how data flow through the infrastructure and

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

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

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
- 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

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

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

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

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

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
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

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

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

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

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

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,

Processor: a natural or legal person, public authority, agency or other body which processes

Recipient: a natural or legal person, public authority, agency or another body, to which the

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

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,

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