RIDER 118
INFORMATION SECURITY
APPLICATION SERVICE PROVIDER ASSESSMENT SURVEY

By signing the Agreement, or accepting the Purchase Order, to which this Rider is attached Contractor affirms, certifies, and warrants that the information set forth in this Rider is current, complete, and accurate. Contractor agrees that in the event Contractor makes a false statement by affirming, certifying, or warranting the information set forth in this Rider, MD Anderson may, at its option, terminate the Agreement/Purchase Order to which this Rider is attached without further liability, and Contractor shall be removed from all MD Anderson bid lists.

Contractor agrees to provide a certificate of assurance to MD Anderson, on or before each anniversary of the Effective Date, certifying that the information set forth in this Rider continues to be current, complete, and accurate and that any updating, testing, or other activities required to be performed on an ongoing or periodic basis have been and are being performed in accordance with this Rider 118. Contractor agrees to notify MD Anderson in writing within thirty (30) days of any changes in the affirmations, certifications, and warranties made by Contractor under this Rider.

The terms "Confidential Information" and "Restricted Confidential Information" are defined as follows:
1) **Confidential Information** is Information that, if compromised, would have a significant financial impact to M. D. Anderson, and violate federal or state law or the terms of confidentiality provisions in MD Anderson contracts. Such information should be accessed only by a limited, authorized group of people. All data sets that contain PHI receive this classification level, at a minimum.
2) **Restricted Confidential Information** builds upon the Confidential classification by addressing special access needs of a subset of PHI, such as mental health data. Restricted Confidential Information should be accessed only by specific authorized people. Only the owner of the data may designate information sets as Restricted Confidential or grant access to this data.

ASP Provider Name: _____ Date: _____
Address : _____ Website: _____
ASP IT Security Contact: _____ Email: _____ Phone: _____
Location of Data Center (DC): Contact: _____ Phone: _____
Ownership of DC Building _____ Geographic Redundancy of DC? YES___ NO ___
Location of Recovery Center: _____ Contact: _____ Phone:_____
Institution's Sponsoring Dept. Information System Security Contact: _____ Phone: _____

SECTION TO BE COMPLETED BY MDACC:

Description of Service/Product: _____

Who are Users of the System? _____

SECTION TO BE COMPLETED BY MDACC:

DATA REQUIREMENTS

(mark a "1" in all boxes applicable for this relationship)

Transmit or Access	Stores Offsite	*Risk*	*Data Type (if needed, refer to definitions worksheet tab)*
		High	Electronic Protected Health Information (ePHI)
		High	Personally Identifiable Information (PII) for Students
		High	Personally Identifiable Information (PII) for Non-students
		High	Social Security Numbers (SSN)
		High	Payment Card Information
		High	Sensitive or Confidential Digital Research Data
		High	Institution Mission Critical Information
		Medium	Business Critical Information
		Medium	Intellectual Property
		Medium	Other Sensitive or Confidential Information
		Low	Other

USE THE KEY BELOW TO ANSWER THE FOLLOWING SURVEY QUESTIONS:

Answer: 0 = Not Applicable, based on service provided
1 = Yes
2 = Partially
3 = No

Comments: are optional, but may be used to explain answers.

Answer	Comments	A. Company Information
		1. Supplier will provide documentation on financial health and viability of the company before contract execution.
		2. Supplier will accommodate a customer's site visit for a security audit within 24 hours notice.
0		***Total Company Controls***

Answer	Comments	Deferrable = compliance within 6 months	B. Policies, Standards and Procedures
			Supplier has formal written Information Security Policies that include the following: *(Answer each subject below that is included in the supplier Information Security Policies)*
			1a. Acceptable Use
			1b. Administrative Access
			1c. Backup of Data and Applications
			1d. Change Management
			1e. Computer Virus Prevention
			1f. Email
			1g. Encryption Requirements
			1h. General Account Management
			1i. Passwords
			1j. Internet Use
			1k. Information Owners Responsibilities
			1l. Server Hardening
			1m. Media Control & Handling
			1n. Identification & Authorizations
			1o. Network Access
			1p. Network Scanning
			1q. Patch Management
			1r. Physical Access
			1s. Portable Computing & Remote Access
			1t. Risk Management Program
			1u. Security Awareness Training
			1v. Security Incident Management
			1w. Workstation Security
			1x. Information Security & Information Oversight Responsibilities
			1y . Information System Administrator Responsibilities
			1z. Management of contracted Resources
			2. Supplier will provide copies of the Information Security Policies upon request.
			3. Supplier will provide, if asked, examples of security documents it maintains as indicated in its Information Security Policies; for example, documentation of security incidents.

			4. Supplier will provide results of a third-party external Information Security assessment conducted within the past 2 years (SAS-70, SOC 2 (Type 1 & 2), penetration test, vulnerability assessment, etc.) upon request.
			5. Supplier maintains and will provide a copy of its incident response procedures.
			6. Supplier has Policy that protects client information against unauthorized access; whether stored, printed, spoken, or transmitted.
			7. Supplier has Policy that prohibits sharing of individual accounts by using unique user name and password to identify and authenticate the individual in order to access data on the Server, Workstation, Application and other device.
			8. Supplier has Policy that implements the following Information Security concepts: need to know, least privilege, and checks and balances e.g., Role-based Access, Rule-based Access, etc.
			9. Supplier receives and implements protections for security vulnerability alerts (such as CERTs).
			10. Supplier requires system administrators to be educated and qualified to perform maintenance of information systems. Supplier will provide Position Description upon request.
			11. Supplier implements AAA (Authentication, Authorization, Accounting) for all users.
			12. Supplier performs personal and criminal background checks for individuals who have access to MD Anderson Confidential Information and Restricted Confidential Information to ensure that employees are eligible to participate in federally funded healthcare programs as well as to stay in compliance with **University of Texas System Policy 124**, Criminal Background Checks for contractors who have access to MD Anderson information resources; access to confidential information; access to currency; access to pharmaceuticals, select agents or controlled substances; and responsibility for care of patients or vulnerable populations.
			13. Supplier has employee termination or job transfer procedures that can immediately be put into effect to protect unauthorized access to information.
			14. Supplier provides customer support with escalation procedures.
			15. Supplier documents its change control processes.
			16. Supplier requires contractors, subcontractors, vendors, outsourcing ventures, or other external third-party contracts to comply with its policies and its agreements with its customers.
			17. Supplier has Policy that implements Federal, State of Texas and The University of Texas MD Anderson Cancer Center regulatory requirements.
		Y	18. Supplier maintains a routine user Information Security awareness program.
		Y	19. Supplier has a formal routine Information Security risk management program for risk assessments and risk management.
0			***Total Policy Controls***

Answer	Comments		**C. Network Architecture**
			1. Supplier will provide a network topology diagram/design upon request.
			2. Supplier Implements firewall protection on their network.
			3. Supplier maintains routers and ACLs (Access Control Lists)
			4. Supplier provides network redundancy.
			5. Supplier has Intrusion Detection System/Intrusion Prevention System (IDS/IPS) technology implemented.
			6. Supplier has Demilitarized Zone (DMZ) architecture for Internet systems.
			7. Supplier has Web applications that 'face' the Internet on a server that is different from the server that contains a database or data with sensitive information.
			8. Supplier has Enterprise virus protection.
			9. Supplier has Enterprise patch management.
			10. Supplier provides dedicated customer servers or explains how this is accomplished in a secure virtual or segmented configuration.
			11. Supplier has remote access that is achieved over secure and encrypted connections.
			12. Supplier has separate physical/logical testing environments.
			13. Supplier provides the architectural software solution design with security controls stated in this ASP Rider.
			14. Supplier has wireless network with controlled and secure access points.
0			***Total Architecture Controls***

Answer	Comments		**D. Configurations**
			1. Supplier will keep all of its computer systems used under this Agreement current with security patches and will take all steps necessary to provide such systems from malware. This applies to the application code that makes up the application; the computer servers that host the applications' operating systems patch plan; all supporting software that is needed for the application to operate; and all database management systems that are used by the application
			2. Supplier has Encryption for sensitive information (protected health information, student identifiable information, personnel information, intellectual property, etc.) for external or Internet transmissions with a strength of at least 128 bit.
			3. For systems that support users, Supplier has banners that display prior to access. These banners notify users that the system is a business system and that usage is monitored and compliance enforced.
			4. For systems that support users, Supplier has computers with password-protected screen savers that activate automatically to prevent unauthorized access when unattended.
			5. Supplier will ensure that the computers it uses under this Agreement do not include or access any software or services that are not necessary for Contractor's performance under this Agreement. If Supplier cannot agree to this, Supplier must define the specific reasons why.
			6. Supplier has changed or disabled all vendor-supplied default passwords or similar "published" access codes for all installed operating systems, database management systems, network devices, application packages, and any other commercially produced IT products.
			7. Supplier requires all passwords to have a minimum of 8 characters, expire, and have strength requirements. Where technically feasible, Supplier requires all administrative passwords have 15 characters, expire, and have strength requirements.
			8. Supplier requires passwords that are never stored in clear text or are easily decipherable.
			9. Supplier has all systems and software checked to determine whether appropriate security settings are enabled.
			10. Supplier has file and directory permissions managed for least privilege and need-to-know accesses.
			11. Supplier has redundancy or high availability features implemented for critical functions.
			12. Supplier has all user access authenticated with either a password, token or biometrics.
			13. Supplier has all system changes approved, tested and logged.
			14. Supplier does not use production data for testing unless the data has been declassified.
			15. Supplier has Application security that follows industry best practices (such as OWASP).
			16. Supplier has account lockout feature that is set for successive failed logon attempts for systems that support users.
			17. Supplier prohibits split tunneling when connecting to customer networks.
0			***Total Configuration Controls***

Answer	Comments		**E. Product Design**
			1. If the product integrates with portable devices or stores sensitive information or information protected by law on portable devices, then Supplier (a) encrypts all data that is stored on those devices and (b) will implement and require secure password access to those devices and the information stored on them.
			2. Supplier ensures that access to any sensitive information or information protected by law that is conducted across a public connection is encrypted with a secured connection and requires user authentication.
			3. Supplier ensures that if the product manages Protected Health Information (PHI), the product is HIPAA compliant.
			4. Supplier ensures that if the product manages any payment card information it is compliant with the Payment Card Industry (PCI) Standards.
			5. Supplier ensures that all Web applications are regularly tested and monitored for common application security vulnerabilities.
			6. Supplier ensures that the application server and database software technologies used are kept up-to-date with the latest security patches.

0		***Total Product Design Controls***

Answer	Comments	F. Access Control
		1. Supplier ensures that, in the event of any termination, transfer, or change in job functions of its personnel, Supplier immediately removes or modifies those persons' access to the products and services it provides under this Agreement as necessary to ensure the security of those products and services.
		2. Supplier achieves individual accountability by assigning unique IDs and prohibits password sharing.
		3. Supplier ensures that critical data or systems are accessible by at least two trusted and authorized individuals.
		4. Supplier reviews all access permissions at least once annually and that such reviews are updated as required for all server files, databases, programs, etc..
		5. Supplier ensures that Users only have the authority to read or modify those programs or data which they need to perform their assigned duties.
0		***Total Access Controls***

Answer	Comments	G. Monitoring
		1. Supplier reviews access permissions according to regulatory requirements based on data content or at least annually for all server files, databases, programs, etc.
		2. Supplier implements System event logging on all servers and records to, at a minimum, record who, what, and when access to such servers and records occurs.
		3. Supplier reviews and analyzes system activities or accesses on at least a bi-weekly basis; provided that at a minimum Supplier performs such reviews on a daily basis for all systems that store, process, or transmit data subject to the PCI Standards.
		4. Supplier reviews system logs for failed logins or failed access attempts on at least the frequency required by regulatory requirements; provided that at a minimum Supplier performs such reviews on a daily basis for all systems that store, process, or transmit data subject to the PCI Standards.
		5. Supplier reviews and removes dormant accounts on systems on at least a monthly basis.
		6. Supplier periodically reviews logs for possible intrusion attempts, conducting such reviews at least according to regulatory requirements; provided that at a minimum Supplier performs such reviews on a daily basis for all systems that store, process, or transmit data subject to the PCI Standards.
		7. Supplier reviews network and firewall logs on at least a bi-weekly basis; provided that at a minimum Supplier performs such reviews on a daily basis for all systems that store, process, or transmit data subject to the PCI Standards.
		8. Supplier reviews wireless accesses on at least a monthly basis.
		9. Supplier routinely performs scanning for rogue access points.
		10. Supplier actively manages IDS/IPS systems and implements alert notifications.
		11. Supplier routinely performs vulnerability scanning.
		12. Supplier routinely performs password complexity checking.
0		***Total Monitoring Controls***

Answer	Comments	H. Physical Security
		1. Supplier ensures that access to secure areas is controlled, including controls such as: key distribution management, paper/electronic logs, or ensuring that a receptionist is always present when the doors to such areas are opened.
		2. Supplier (1) ensures that access to server rooms is controlled and (2) follows need-to-know and least privilege concepts in controlling access to such rooms.
		3. Supplier ensures that all computer rooms have special safeguards in place i.e., cipher locks, restricted access, room access log.
		4. Supplier ensures that printed confidential or sensitive information is disposed of in a secure manner (e.g., shredded or otherwise destroyed securely.)
		5. Supplier either (1) prohibits customer information (PHI, student data, SSN, etc.) from being stored on laptop computers or other portable devices or (2) only allows customer information to be stored on laptop computers or other portable devices if encrypted.
		6. Supplier ensures that all desktops that display Confidential Information are positioned to prevent unauthorized viewing of such information.
		7. Supplier requires all visitors to be escorted in computer rooms or server areas.
		8. Supplier has implemented appropriate environmental controls where possible to manage equipment risks such as: alarms, fire safety, cooling, heating, smoke detector, battery backup, etc..
		9. Supplier ensures that there are no external signs at its facilities indicating the content or value of the server room or any room containing sensitive information.
		10. Supplier implements secure processes for destroying sensitive data on hard drives, tapes or removable media, so that such data is no longer recoverable by any means once so destroyed.
0		***Total Physical Controls***

Answer	Comments	I. Contingency
		1. Supplier maintains and implements a written contingency plan for mission critical computing operations.
		2. Supplier maintains emergency procedures and responsibilities that are documented and stored securely at multiple sites.
		3. Supplier reviews, tests and updates its contingency plan at least annually.
		4. Supplier has identified what computing services must be provided within specified critical timeframes in case of a disaster.
		5. Supplier has identified cross-functional dependencies so as to determine how the failure in one system may negatively impact another one
		6. Supplier has written backup procedures and processes.
		7. Supplier periodically tests the integrity of backup media.
		8. Supplier stores backup media in a secure manner and ensures that access to such media is controlled.
		9. Supplier maintains a documented, tested, and updated disaster recovery plan and reviews such a plan at least annually in collaboration with MD Anderson data owners.
		10. Supplier has off-site storage and documented retrieval procedures for backups.
		11. Supplier has rapid access to backup data.
		12. Supplier has backup media that is appropriately labeled to avoid errors or data exposures.
0		***Total Contingency Controls***

Answer	Comments	J. Business Relationships
		1. Supplier ensures that confidentiality agreements are signed by its employees, contractors, agents, and others before Supplier discloses proprietary and/or sensitive information to them.
		2. Supplier ensures that business associate contracts or agreements that contain appropriate risk coverage provisions meeting the requirements of Supplier's customers are in place before work starts.
		3. Supplier ensures that its business associates are aware of customer security policies and what is required of them under such policies.
		4. Supplier ensures that its business associates agreements include provisions for protection of a customer's data by the business associate and address the business associate's return or destruction of such customer data when the relationship terminates.
0		***Total Business Relationships Controls***

0		***TOTAL CONTROL SCORE***