**Data Security and Governance -** ***Information Security and Access Control***

The proposed solution must adhere to federal and state regulations (FERPA, HIPAA, GDPR, Graham-Bliley Act, etc.) as well as to Lander's Information Technology Service (ITS) policies and procedures with regards to data protection and privacy, firewalls, email and access policies and procedures.

If modifications or additional costs are needed for the solution to meet any referenced requirement, detailed costs of services, products and components must be listed or attached to the proposal.

**Requirements:**

a. Describe offeror's business continuity and disaster recovery plans.
b. If implemented, single sign-on must be Azure-ADFS compatible.
c. Data encryption must be accommodated in transit and "at rest".
d. The equipment hosting the solution for the University must be located in a physically secure facility and within the boundary of the Continental United States of America.
e. Describe physical security practices for hosted or cloud-based solutions.
f. Provide offeror's procedures for data and system access, data retention, disposal and replacement of hard drives and disposal of backup tapes.
g. Is Offeror's system in a shared environment? Will Lander have a dedicated system or instance of Offeror's solution? What are offeror's firewall port requirements for cloud-based solutions?
h. Please describe privacy policy.
i. Does offeror have specific IP's that can be matched to firewall rules?
j. If the system to be integrated with Lander systems (e.g., Ellucian Colleague, SSO, etc.), what are the required IT resources and hours during the initial implementation and thereafter? Please describe and state in details the types of IT resources required, initial and ongoing required hours to implement and support the solution.
k. Describer Offeror's termination or exit process for ensuring successful transition to an alternative solution.
l. Must adhere to the University's Information Technology Service (ITS) policies and procedures with regards to firewalls, email, domain and access policies and procedures as well as industry best standards.
m. The solution must natively handle email capabilities and adhere to industry best practices.
n. The solution must be PCI-DSS (latest industry acceptable version) Compliant with P2P encryption devices.
o. The solution must use SC State contract merchant services processor and compatible payment gateway (e.g., TouchNet, First Data/SunTrust).
p. The solution must have the ability to securely export monthly credit card payment details into an Excel worksheet from the solution.
q. The solution must be P2PE certified POS (point-of-sale) devices for in-person credit/debit card transactions with EMV capability.
r. SRED keypads or secure device to process telephone payments without inputting credit/debit card numbers into Lander computer keyboards.
s. Attestation of Compliance to PCI-DSS Standards to the university on an annual basis.
t. How does the solution provide levels of role-based security?
u. How does the solution handle logging/auditing capabilities (internally and externally)?
v. What measures are in place to protect against web security flaws such as SQL injection, XSS, broken authentication and session management?
w. Does the offeror have an established information security program (that adheres to applicable Federal, and State regulations and Information Security standards, guidelines, and best practices) to fully address confidentiality, integrity and availability of data? Can a copy of the IS Program be provided to Lander, including auditing by an independent entity?

**Data Governance and Security - *<u>Information Security Data Elements Checklist</u>***

Lander requires that third-party contractors and partners protect and safeguard University information or information that’s entrusted to the University. All contractors who transmit, access, process or store compliant data are required to agree to federal, state regulations as well as industry standards/best practices and Lander’s standards and policies.

| | |
|---|---|
| 1. Will the offeror as a third party be: (Please Check all that apply) | ☐Transmitting<br>☐ Accessing<br>☐ Processing<br>☐ Storing University Data |
| 2. How many records will be involved? | ☐ 250<br>☐ 251-500<br>☐ 501-1000<br>☐ 1000+ |
| 3. Data elements to be transmitted, accessed, processed or stored by the Offeror. | ☐ Social Security Numbers<br>☐ Driver’s License Number or State<br>☐ Identification Card Number<br>☐ Personal Financial Information:<br>Account #, Account Password,<br>☐ Personal Identification Number (PIN)<br>☐ DOD classified data, or special Sensitive Data<br>☐ Protected Health Information (PHI)<br>☐ Covered by insurance.<br>☐ Payment card data (credit or debit card)<br>☐ We will be using a third-party merchant account.<br>☐ Unsure what merchants will be used.<br>☐ Student information FERPA data or directory information that students have opted not to have released.<br>☐ Academic evaluations such as tests, scores, and transcripts.<br>☐ General counseling/advising records.<br>☐ Disciplinary records.<br>☐ Financial aid records, including loan collection records.<br>☐ Disability status/medical issues.<br>☐ Which SAQ does the offeror fill for PCI-DSS compliance?<br>☐ Any other University non-public data (Compliant or Business Sensitive) not shown above. Please Provide Examples: |

***Accessibility Requirements:***

Since the solution would have end-user human interface (e.g., end-user device software component, web pages or sites, mobile device components, etc.), the offeror must submit one or both of the following assessments that users, instructors, system administrators, etc., are expected to interact with.

1. A current and accurate "Voluntary Product Accessibility Template", or VPAT, (see http://www.itic.org/public-policy/accessibility), to document products and/or services' conformance and deviations from Section 508 of the Rehabilitation Act of 1973.
2. A detailed description of the accessibility features that shows and explains compliance with and deviations from the guidelines of the "Web Content Accessibility Guidelines (WCAG) 2.0" published by www.w3.org.

**General Information Technology Questionnaires:**

The system requirements should reflect delivered/"out-of-the-box" functionality. Offerors must indicate if modifications, additional product costs or if any other accommodations would be necessary to meet any of the requirements. Additional costs, customizations or upgrades must be provided, detailing the costs and item descriptions. Costs will include any one-time/initial costs as well as ongoing annual support costs.

| | |
|---|---|
| 1. SaaS/hosted/cloud solutions | a. Please list normal scheduled downtime frequency, uptime percentage, standard day/time openings, etc.<br>b. Please describe the minimum desktop workstation hardware and software requirements required by the solution.<br>c. Please describe details of network communications required between the solution and other solution including University systems.<br>d. Please describe deployment instances of the environment (e.g., test, development and production). Are all of the instances available to Lander? If yes, detail the types of instances and how access would be provided.<br>e. Please reference the vendor SLA (Service Level Agreement) support requests. |
| 2. Solution components that are provided by third-party partners, including OEM software, hosting, internal application network, etc. | a. Please describe the main technologies for the components.<br>b. Please provide third-party technology partner(s) name(s), address(es) and contact(s).<br>c. Please explain additional costs or fees associated with the referenced components. |
| 3. Practices and policies related to data stored by this solution | a. Please describe how data will be "completely erased" upon the contract termination.<br>b. Please clarify data ownership rights and responsibilities of the parties and provisions for Lander obtaining the data as needed.<br>c. Please indicate types of data stored especially if any data is protected (e.g., HIPAA, FERPA, |

| | |
|---|---|
| | etc.).<br>d. Please indicate how long data is stored or archived.<br>e. Please describe the technology, practices and policies you have in place that would protect Lander data from unauthorized access and use.<br>f. Please indicate how full data sanitization is completed to ensure the integrity of imported data? |
| 4. Business continuity and disaster recovery management practices | b. Please describe the strategies to minimize downtime in the event of a catastrophic failure of the hosting environment(s) or components.<br>c. Would Lander experience any loss of data as a result of downtime, system problems or catastrophic failure? If yes, describe the situations that could result in loss of Lander data.<br>d. How much downtime should Lander expect for a catastrophic failure? |
| 5. Provide detailed information regarding browser requirements for the proposed solution to meet the functionality and system requirements, including any specific required versions and/or add-ins. | |
| 6. Describe the mobile capabilities available with the proposed solution | a. Please indicate supported mobile platforms.<br>b. Please describe implementation of mobile capabilities (i.e. mobile-enabled, apps, etc.)<br>c. Please explain how and when mobile updates provided.<br>d. Please explain how you ensure that all mobile interfaces to your solution comply with disability accessibility requirements such as Section 508 and/or WCAG2.0. |
| 7. Does the solution provide data exports for upload to Lander systems? If so, please describe the types of information exported and the process employed. | |
| 8. Can the solution automate data importing and exporting? | |
| 9. Does the solution come with a comprehensive data dictionary of the database? | |
| 10. Identity Management System | a. If the solution integrates with identity management systems, please describe the delivery mechanism of this component.<br>b. Does the solution offer capabilities to use Azure ADFS?<br>c. Please describe the SSO implementation requirements.<br>d. Does the solution deliver an API that would allow for the remote management of user authorization data? If yes, please describe how. |
| 11. Please describe the ongoing functions to be performed by Lander system and application administrators?<br>12. Does the solution need a full-time staff member to be administered and maintained? | |
| 13. What is the maximum number of logged in concurrent users can the solution support? How does the system define concurrent users? | |

| | |
|---|---|
| ***Data Governance and Security - Interface Data Exchange Requirements:*** | |
| Transfer of data will must be accomplished only via using secure methods such as, but not limited to HTTPS and SSH/SFTP. Offerors must provide secure file transfer solutions and may recommend alternative processes if they would be beneficial to Lander. Alternatives must be described in detail and are subject to Lander's approval. For all proposed transmission methods, the offerors must provide the technical requirements, processing transactions, a detailed description of security and authorization processes and requirements, forms, encryption or authentication requirements, and devices or digital certificates, alternatives available if the standard transmission method fails, plus a disclosure on any software limitations on file sizes or numbers of records in a batch.<br>Requirements should reflect delivered/”out-of-the-box” functionality. Offerors must indicate if system modifications, additional product or costs or if any other accommodations would be necessary to meet any requirement. Additional costs customizations or upgrades must be provided in details. | |
| ***Technical Interface Data Exchange:*** | |
| 1. The proposed solution must interface with an online payment processing gateway for eCommerce services such as online payments. The proposed solution must be able to interface seamlessly with the University’s payment card processor TouchNet payment systems and compatible with payment platforms if needed. | a. Is the proposed solution an existing TouchNet partner?<br>i. Can the solution integrate with the TocuhNet platform at the Offeror’s expense? A time frame for accomplishing this integration must be provided.<br>ii. Does the solution currently have an existing website for accepting payments? If so, please provide that URL and assurances that it is PCI-DSS compliant.<br>iii. Does this solution use a third-party application for accepting payments? If so, who is the third-party service provider of the application, and provide assurance that the application is PA-DSS compliant.<br>b. What other Payment Gateways does the Offeror partner with (e.g. FirstData, etc.) |
| 2. If integration with University ERP (Ellucian Banner) is requested, is there an existing/”out-of-the-box interface with the ERP, or would a custom interface need to be developed? Please provide details of any additional costs for seamless integration. | |
| 3. Does the solution allow easy secure integration with other applications including desktop tools (i.e. Microsoft Office Professional Suite (Word, Excel, PowerPoint, Access Dataset)? | |
| 4. Does the solution provide for auto/mass load of new and existing records (including ID records), matching on IDs where necessary (non-ID records) to obtain data from external sources? Users MUST be able to perform the load, preview it online, and set additional rules before committing it to the database. It is preferable that a wizard or other user aid be available for this purpose. Some "uploads" may be updating existing records. | |