Procurement and Contracting Services

Request for Proposals for a Student Response System

ADDENDUM #1

Please mark all proposal submission
Envelopes with the following information

Sealed RFP # L192315
Due on February 15, 2023 no later than 2:00 PM, MST

The following questions were received prior to the close of the Technical Question period on February 1, 2023 at 12:00 PM MST:

1. Assuming we are able to accept the provided terms, are we able to provide supplemental/additional terms of our own?
   a. You are welcome to submit any additional terms, but acceptance of a response does not mean acceptance of the additional terms. The University would expect to negotiate upon award.

2. Given the multi-year nature of the provided agreement, does the university expect to maintain approximately 47,000 FTE over the next 5 years?
   a. Yes. If it changes dramatically due to the consolidation of UAGC then we will in good faith update the FTE number and proceed with adding the per unit cost of each student FTE.

3. Regarding the submission of the requested documents, my team plans to structure said submission as follows:
   a. 1 uploaded PDF document containing answers to the requested information from sections 5.3-6.4 within the RFP, supplement information/functionality of Poll Everywhere, requested referrals and signatures.
   b. The provided Attachment A, completed

      i. Is this format for submission acceptable?

      This format is acceptable but please make sure to include a redacted copy of the response if you deem certain information as confidential, keeping section 3.8.3 in mind.

4. Where can I find the Information Security and Privacy Addendum?
   a. Please see the end of the addendum. The Information Security and Privacy Addendum is attached.

5. In section 5.0, there is a statement requesting the Student Response System support the university's learning ecosystem's integrations. Can you describe the required learning ecosystem integrations and the use case(s) between those integrations and the student response system?
   a. Current ecosystem is Brightspace(D2L) and Shibboleth (SAML) Single Sign On. We would hope that the Brightspace integration would include rostering, user creation, role authorization in alignment with IMS Global Roles (Student and Instructor in LTI), and gradebook integration for updating scores. Please describe your gradebook integration.

6. Approximately how many unique students use some type of student response system on campus or remotely?
   a. 30,000 unique users leverage this technology.

7. Approximately how many faculty use a student response system with their curriculum?
   a. 400 annually

8. What University of Arizona colleges or schools have not adapted the use of a student response system?
    a. Faculty usage is present in almost all colleges and is expected to be used in all colleges as a result of this RFP.

9. Would you like simply a list of references or to include a testimonial from the contact about their work with the vendor?
    a. List of references with contact information for people that we can contact.

10. What format would you like the answers to the Scoring Criteria in? We are happy to answer within the excel doc or in a separate word document where graphics and screenshots can be included.
    a. Excel file.

11. Section 5.5 Accessibility: These questions are listed in both Attachment A and Section 5. Would you like vendors to answer these questions in both locations or is one or the other preferred?
    a. Both is preferred. At least in Attachment A.

12. Section 4 question 20: Implementation and support: “Provide a description of your support levels based on ticket severity, and the response time for each level?”
    a. Please provide your Service Level Agreement documentation.

13. Question: Is the description/response time requested pertaining to support tickets or bugs, or both?
    a. Both.

14. May we get an extension on the due date of the RFP?
    a. No.

15. Will UofA accept a Canvas LTI integration?
    a. No. We are currently a Brightspace school and require a Brightspace or LTI integration. If your LTI integration does not support scores moving to the gradebook then please be transparent and say that.

16. Is there a budget threshold?
    a. There is no threshold, but it is included in the scoring criteria and is considered as part of finding the best solution.

17. Is there any interest in sharing poll data across multiple courses, departments, Colleges, or at the University wide level?
    a. Yes, we would like to be able to retrieve our data that is stored in your system on a daily or weekly basis as we want to merge it with our data warehouse as part of identifying students at risk.

University of Arizona Information Security and Privacy Addendum

This Information Security and Privacy Addendum ("ISPA") is between the Arizona Board of Regents on behalf of The University of Arizona ("University") and [VENDOR] ("Vendor") and is hereby incorporated into the Agreement between the parties dated [DATE] (the "Agreement"). Vendor is providing [description of services] (the "Services"), and by doing so, add the following terms and conditions as an addendum.

1. **Definitions** Capitalized terms used but not defined in this ISPA have the same meanings as set out in the Agreement.

Cloud Software means any externally hosted technology offering which enables on-demand Network access to a shared pool of configurable computing resources.

EEA means the European Economic Area (including the United Kingdom).

Medical Records means all communications related to a patient's physical or mental health or condition that are recorded in any form or medium and that are maintained for purposes of patient diagnosis or treatment, including medical records that are prepared by a health care provider or by other providers.

Network means any University network to which Vendor is provided access in connection with the performance of Services under the Agreement and/or any Vendor network that may access University Data.

Process or Processing means 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.

Personal Information means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual, device, or household.

Security Incident means any accidental, attempted, unlawful, or unauthorized destruction, alteration, disclosure, misuse, loss, theft, access, copying, modification, disposal, compromise, or access to University Data or any act or omission that compromises or undermines the physical, technical, or administrative safeguards put in place by Vendor in Processing University Data or otherwise performing the Services.

System means any desktop or laptop, mobile device, server and/or storage device that, (i) is involved in the performance of the Services, (ii) may be used to access a Network, or (iii) may access or store University Data.

University Data means any and all data, information, text, graphics, works, and other materials that are collected, loaded, stored, accessible, transferred through and/or accessed by Vendor or provided to Vendor by University. This includes University's Systems and Network and also includes, but is not limited to: (1) all of the deliverables, reports, or materials from the Services; (2) all University information and materials that Vendor develops or acquires prior to, or independently of, the Agreement; (3) and any Personal Information or Medical Records pertaining to University end users, students, staff, patients or any other individuals identified in materials provided to or made accessible to Vendor by University. University Data is Confidential Information.

2. **Restrictions on University Data Use**

a. Vendor represents and warrants that it will only collect, access, use, maintain, and Process University Data for the sole and exclusive purpose of providing the Services in the Agreement, and may not retain, collect, use or disclose the University Data for any purpose other than performing the Services. Vendor may not share or sell the University Data for any reason or disclose the University Data to any third party except to provide the Services specified in the Agreement.

b. Upon termination or expiration of the Agreement or upon written request from University, whichever comes first, Vendor will, and will ensure that its Representatives (as defined below), immediately cease all use of and return to University or, at the direction of University, destroy all such University Data provided under this Agreement. If University elects for destruction, Vendor must certify to University that such University Data has been destroyed. If Vendor is required by law to retain any University Data, Vendor must notify University of such requirement and will maintain the confidentiality of such University Data and may not use University Data for any purpose other than as required by law.

c. Vendor will limit access to University Data to its employees, contractors, subcontractors, and/or agents ("Representatives") whose access is necessary to carry out the Services and will ensure those Representatives to keep all University Data confidential. Vendor will inform all Representatives of the confidential nature of University Data and all Representatives will be bound by confidentiality agreements with similar or greater confidentiality and security obligations as Vendor provides to University in the Agreement. Vendor agrees to be legally and financially liable for any breach of this ISPA, or unauthorized disclosure or misuse of University Data by its Representatives. The access rights of any Representatives will be removed immediately by Vendor upon termination or adjusted when such access is no longer necessary. Unless expressly consented to by University, Vendor will host and only allow access to University Data in the United States.

d. If Vendor and its Representatives will have access to University Data, Systems, or Networks, Vendor must ensure that its Representatives have undergone annual privacy and security training and adhere to Vendor's policies and procedures that relate to privacy and security.

e. If Vendor is contacted by a third party with a request, inquiry, or complaint regarding University Data, Vendor will promptly (a) and in any event within two (2) calendar days, provide University with written notice of such request,

inquiry or complaint to security@arizona.edu; and (b) provide University all reasonable cooperation, assistance, information and access to such data in its possession or control as is necessary for University to respond to such request, inquiry or complaint. Vendor will not respond to such request, inquiry or complaint unless so instructed in writing by University.

3. **Written Information Security Program**

a. At all times during the term of the Agreement, Vendor will implement and maintain a written information security program ("WISP"), which must include appropriate administrative, technical, physical, and operational safeguards to maintain the security, privacy, availability, integrity, and confidentiality of University Data in use, in motion, and at rest.

b. Vendor will implement and maintain a formalized risk governance plan, policy, and a continuous risk assessment process demonstrating Vendor's ability to identify, quantify, prioritize, and mitigate risks. If requested by University, Vendor will (and/or cause subcontractors to) certify its compliance with the requirements of this ISPA and provide written responses to any reasonable questions submitted to Vendor by University. Vendor agrees to conduct and provide to University a Data Protection Impact Assessment ("DPIA") or an independent audit report, if reasonably requested by University.

4. **Data Privacy and Security**

a. Vendor agrees to implement and maintain administrative, technical, physical, and operational safeguards in accordance with industry best practices at a level sufficient to secure University Data.

b. Vendor agrees to maintain the following enterprise controls for any Networks or Systems that host, Process, or provide access to University Data:

i. Asset and Information Management. Vendor will maintain and enforce policies and controls that include, without limitation, asset inventory/management, encryption (in transit and at rest), storage of data on portable hardware, and third-party access to and use of University Data.

ii. Human Resources Security. Vendor will maintain and enforce a policy that addresses human resources security for all Representatives accessing University Data. Vendor will conduct background checks and not utilize any individual to fulfill the obligations of this Agreement if such individual has been convicted of any crime involving dishonesty or false statement including, but not limited to fraud and theft, or otherwise convicted of any offense for which incarceration for a minimum of one (1) year is an authorized penalty. Any such individual may not be a "Representative" under this Agreement

iii. Physical Security. All facilities used by or on behalf of Vendor to store and process University Data will implement and maintain administrative, physical, technical, and procedural safeguards in accordance with industry best practices at a level sufficient to secure University Data from a Security Incident. Such measures will be no less protective than those used to secure the Vendor's own data of a similar type, and in no event, less than reasonable in view of the type and nature of the data involved.

iv. Data and System Access Controls. Vendor will maintain and enforce policies and controls that include, without limitation, role-based permissions for access to University Data (using a principle of minimization), restrictions on copying or removing data from an authorized network or system, strong password protocols (i.e., complexity requirements, mandatory changes, restrictions on sharing, etc.), and multi-factor authentication or equivalent protections for any remote access to Vendor's network or systems. Vendor will trace approved access to ensure proper usage and accountability, and the Vendor will make such information available to the University for review, upon the University's request and not later than five (5) business days after the request is made in writing.

v. Availability Control. Vendor will take industry-standard steps to ensure that University Data is available when requested by University. Additionally, Vendor must take steps to protect against accidental destruction or loss of University Data, including, without limitation, anti-virus software; firewalls; network segmentation; user of content filter/proxies; interruption-free power supply; threat detection and prevention; regular generation of and testing of back-ups; hard disk mirroring where required; fire safety system; water protection systems where appropriate; business continuity and emergency plans; and air-conditioned server rooms.

vi. Network Security. Vendor will carry out updates and patch management for all systems and devices in a timely manner, applying security patches within five (5) business days or less based on reported criticality. Updates and patch management must be deployed using an auditable process that can be reviewed by the University upon the University's request and not later than five (5) business days after the request is made in writing. An initial report of patch status must be provided to the University prior to the effective date of the Agreement. Vendor will maintain documented operating procedures and technological controls to ensure the effective management, operation, and security, of Vendor's Network, including, without limitation, an up-to-date Network diagram, wireless encryption protocols, and adequate remote access protocols.

vii. Logging and Monitoring. Vendor will comply with relevant security best practices for the monitoring and logging of its Networks, applications, and Systems. Logs will be kept for the duration of the Agreement or

Vendor's record retention policy, whichever is longer.

viii. Change Management and Web Applications. Vendor will use secure development and coding standards in accordance with industry standards. Vendor's web applications must meet OWASP Application Security Verification Standards (ASVS). Vendor will perform adequate testing prior to releasing updates, modifications, or new functionality to software.

5. **Representations and Warranties**

a. Vendor represents and warrants that: (i) it will comply with the requirements under applicable privacy and data security laws (including, if applicable, the General Data Protection Regulation (GDPR), Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), Gramm–Leach–Bliley Act (GLBA aka Financial Services Modernization Act of 1999), the Children's Online Privacy Protection Act (COPPA), and/or Payment Card Industry Data Security Standard (PCI DSS)), and applicable state privacy and security laws; (ii) it will comply with the requirements of this ISPA, and (iii) it will perform the Services in accordance with industry standards and in a professional and workmanlike manner. If the Agreement requires or permits Vendor to access, receive, or release any student records, then, for purposes of this Agreement only, University designates Vendor as a "school official" for University under FERPA, as that term is used in FERPA and its implementing regulations.

b. If Vendor is provided access to Medical Records, but the applicable information is not subject to HIPAA, Vendor represents and warrants that it will (i) comply with 16 C.F.R, Part 318 and (ii) only use or disclose Medical Records as permitted or required under the Agreement, or as required by law. At all times during the course of the Agreement, Vendor will make any Medical Records available to University for access, portability, modification, or deletion.

c. Vendor represents and warrants that all responses to any security assessment by University are accurate and truthfully represents the security practices of Vendor. Vendor agrees that, at the request of University, it will provide sufficient evidence of its compliance with obligations set forth in this ISPA.

6. **Data Security Incident**

a. Vendor will maintain, update and document an Incident Response Plan ("IRP"), and will manage, document, review, investigate and resolve all Security Incidents in accordance with the IRP.

b. Vendor agrees to notify University of a Security Incident at security@arizona.edu as soon as reasonably practicable and without undue delay. Such notice must include (i) a description of the incident, including the type of incident (e.g., theft, loss, improper disclosure, unauthorized access), location of the incident (e.g., laptop, desktop, paper), how the incident occurred, the date the incident occurred, and the date the incident was discovered; (ii) a description of the type of University Data involved (e.g., user data, intellectual property, etc.); (iii) a description of the potentially impacted individuals; (iv) a description of the actions taken in response to the Security Incident (e.g., additional safeguards, mitigation, sanctions, policies, and procedures); and (v) all other information reasonably requested by University or necessary to provide notice to individuals and/or regulators, including a forensic report summarizing the findings of a forensic investigation. University acknowledges that certain information may not be immediately available and can be provided on a rolling basis as it is discovered (within 72 hours of discovery).

c. In facilitating the investigation and remediation of a Security Incident, Vendor will cooperate fully with University. Vendor may not inform any third party of any Security Incident without first obtaining the University's written consent, except as may be required by law. Vendor agrees to reimburse University for reasonable costs and expenses incurred (including legal fees) in responding to, remediating, and/or mitigating damages caused by a Security Incident or in following up on a complaint by an individual or a regulator. Vendor will take all necessary and appropriate corrective actions, including as may be reasonably instructed by University, to remedy or mitigate any Security Incident.

7. **Audit and Testing**

a. Vendor will complete one of the following audits at least annually and immediately after any actual or reasonably suspected Security Incident: SOC 2 Type II, SOC for Cybersecurity, or an accepted Higher Education Cloud Vendor Assessment Tool (https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit). Evidence must be provided to the University prior to this Agreement and at least annually thereafter.

b. Prior to this Agreement, and at regular intervals of no less than annually and whenever a change is made which may impact the confidentiality, integrity, or availability of University Data, and in accordance with industry standards and best practices, Vendor will, at its expense, perform scans for unauthorized applications, services, code and system vulnerabilities on the Networks and Systems used to perform Services related to this Agreement ("Security Tests"). An initial report must be provided to the University prior to this Agreement. Vendor will provide the University the reports or other documentation resulting from the audits, certifications, scans and tests within five (5) business days of Vendor's generation or receipt of such results. If any critical finding is identified, Vendor agrees to notify the University and remediate the critical finding within thirty (30) days. Any critical finding not remediated within thirty (30) days must be reported to University at security@arizona.edu. All other findings must be remediated within ninety (90) days. At University's request, Vendor will promptly provide written attestation that required Security Tests, independent audits, and/or a DPIA have been conducted either by a qualified Representative or by a third party in the prior twelve (12)

months. The University may require the Vendor to perform additional audits and tests, the results of which will be provided to the University within five (5) business days of the Vendor's receipt of such results.

c. Vendor agrees to take reasonable steps to assist University in maintaining the accuracy of such University Data under the control of Vendor, including synchronizing relevant Systems, databases, or applications, as deemed necessary by University. The University reserves the right to, at a minimum, an annual, review of: Vendor's access reports related to access to University Data; Vendor's patch management process, schedules, and logs; findings of vulnerability scans and/or penetration tests of Vendor Systems; and Vendor development standards and processes.

8. **International Transfers**

a. If University provides its written consent for Vendor to transfer Personal Information from EEA countries to countries outside the EEA, the terms set out in the EU Standard Contractual Clauses will apply. The parties will work in good faith to populate appendices 1 and 2 of the EU Standard Contractual Clauses and attach an executed version to this ISPA. Vendor agrees to comply with all obligations imposed on a "data importer" set out in such EU Standard Contractual Clauses. For countries located within the Asia Pacific region, Vendor must obtain University prior written consent where Personal Information will be transmitted by the Vendor outside the country from which it was originally collected.

9. **Insurance**

a. Without limiting any liabilities or any other obligation of Vendor, Vendor will purchase and maintain (and cause its subcontractors to purchase and maintain), until all of their obligations under the ISPA have been discharged or satisfied, insurance against claims that may arise from or in connection with the Services, as described here: https://risk.arizona.edu/sites/default/files/InsuranceRequirements5_12_2020.pdf

b. Vendor's Technology Professional Liability Errors & Omissions policy must include Cyber Risk coverage and Computer Security and Privacy Liability coverage with a limit of no less than $2,000,000 per occurrence and $4,000,000 in the aggregate. This policy will provide for both first- and third-party costs, and name University as an additional insured with respect to the provision of Services. This policy will include a waiver of subrogation against University.

c. The required insurance coverage set forth above will not be construed as a limitation or waiver of any potential liability or obligation of Vendor in the Agreement. Failure to maintain the insurance coverage identified in this Section will constitute a material breach.

10. **Appendices**

a. If Vendor is a Cloud Software provider, then the Cloud Software Appendix will apply.

b. If Vendor is processing credit or debit card transactions on behalf of University, the PCI Appendix will apply.

c. If Vendor is collecting, accessing, acquiring, or otherwise Processing Protected Health Information (as defined in the Health Insurance Portability and Accountability Act of 1996), then the PHI Appendix/Business Associate Agreement will apply.

11. **Miscellaneous**

a. Vendor's obligations under this ISPA will survive the termination or expiration of the ISPA and will apply so long as Vendor may access or be in possession of University Data, Network, or Systems. Any requirements imposed on Vendor in this ISPA shall apply to any of Vendor's subcontractors. Following the termination of the Agreement for any reason, Vendor agrees to provide transition services for the benefit of University, including a month-to-month extension (not to exceed ninety (90) days) for the continued provision of its Services and reasonable assistance with the transfer of University Data. The parties agree to take such reasonable actions as are necessary to amend this ISPA from time to time as is necessary for the parties to comply with applicable privacy laws. In the event of inconsistency between the Agreement and the ISPA, the ISPA will govern.

The parties have executed and delivered this ISPA effective as of [Date].

The University of Arizona	**Vendor**
By:_____	By:_____
Name:_____	Name:_____
Date:_____	Date:_____

Cloud Software Appendix

In addition to the terms in the ISPA, the following terms will apply if the Services provided under this Agreement are provided to University as Cloud Software.

1. **Vendor Obligations.** In addition to any other obligations of Vendor, Vendor must:
    a) Provide the Services on a continuous basis and warrants that the Services will be fully available 99.9% of each month, except for scheduled maintenance for which written notice has been provided to University at least thirty (30) calendar days in advance.
    b) Provide unlimited telephone support twenty-four (24) hours a day, seven (7) days a week, three hundred sixty-five (365) days a year ("24/7/365").
    c) Provide online access to technical support bulletins and other user support information and forums 24/7/365;
    d) Conduct quarterly support updates and reviews involving technical teams from both Parties to discuss Cloud Software support issues.
    e) Provide semi-annual support usage, incident reports and Vendor's compliance with any service levels identified in a service level agreement.
    f) Respond with support to Priority One Issues (as defined below) within one (1) hour of University's call for assistance to Vendor and initiate work on such issues within one (1) hour thereafter, regardless of time of day or day of week. Priority One Issues include issues involving substantial failure of the Cloud Software, which, in University's sole judgment, are critical to its operations. Vendor will initiate work on all other support issues, within four (4) hours from receipt of an electronic or telephonic service request.
    g) In the event two or more Priority One Issues occur in any thirty (30) day period during the term of the Agreement, Vendor will promptly investigate the root causes of such support issues and will provide to University an analysis of such root causes and a proposed corrective action plan for University's review, comment and approval (the "Corrective Action Plan"). The Corrective Action Plan must include, at a minimum: (i) a commitment by Vendor to University to devote the appropriate time, skilled personnel, systems support and equipment, and/or resources to remedy, and prevent any further occurrences of Priority One Issues; (ii) a strategy for developing any programming/software updates, fixes, patches, etc. necessary to remedy, and prevent any further occurrences of such issues; and (iii) time frames for implementation of the Corrective Action Plan. There will be no additional charge (other than those fees set forth in this Agreement) for Vendor's implementation of such Corrective Action Plan in the time frames and manner set forth in the Corrective Action Plan.

2. **Scheduled Maintenance of Cloud Software.** Scheduled maintenance, updates, enhancements or modifications relative to the Services and/or other elements or components of the Services will be in accordance with Vendor's maintenance schedule and will not in any way diminish the benefits, comprehensiveness, features or functionality of the Services, as defined under the Agreement. Vendor may, however, push updates and fixes at any time to University that Vendor determines will not affect University's ability to access the Services. Unless otherwise agreed in writing, non-peak hours are from Friday night at 11:00 p.m. MST through Saturday morning at 8:00 a.m. MST, and Saturday night at 11:00 p.m. MST through Sunday morning at 8:00 a.m. MST.

3. **Unscheduled Maintenance of Cloud Software**. If the Services provided under this Agreement are provided to University as Cloud Software, Vendor will provide University with at least seventy-two (72) hours prior notice of Vendor's implementation of all unscheduled maintenance, updates, enhancements, modifications and/or other circumstances which will result in an outage or an inability of University to access the Services. In the event emergency maintenance of the Services is required, Vendor will provide University with as much

advance notice as possible of the impending emergency maintenance and will disclose to University, in writing, the cause or issue necessitating the emergency maintenance as soon as possible and no later than seventy-two (72) hours after the initiation of the emergency maintenance.

4. **Critical Services Not to be Abandoned.** Vendor acknowledges that the Cloud Software provided under this Agreement are critical services for University. Accordingly, notwithstanding any other provisions under the Agreement to the contrary, the Parties agree that Vendor may not "**Abandon"** such critical Services. For purposes of an Agreement, "Abandon" means Vendor's actual, willful non-performance of any material aspect of the Services in breach of the Agreement which results in a material adverse effect on (i) critical aspects of University's internal operations, regulatory or other reporting requirements; or (ii) a Service that is provided to or in support of University's students and faculty. Abandonment will not be deemed to have occurred if non-performance is caused by circumstances outside of Vendor's control or if a Service is properly terminated in accordance with Vendor's rights under the Agreement. In addition, support provided under this Agreement will not be withheld due to any unrelated dispute arising under this Agreement, another agreement between the Parties, or any other unrelated dispute between the Parties.

5. **Public Cloud.** Vendor will not create a public cloud account on behalf of University without prior written approval by University's IT Security team.

6. **Cloud Management.** Vendor is responsible for continuous vulnerability management of hardware and software, including, without limitation, scanning and issue remediation. Vendor is responsible for all disruptions and damage caused to any University Data while it is hosted in Cloud Software.

7. **Hosting Facilities.** University may select or restrict where University Data will be stored and where University Data can be Processed, and the Vendor will store and/or Process it there in accordance with the service terms. If a data location selection is not covered by the service terms (or a data location selection is not made by University with respect to any University Data), the Vendor will default to a United States-based data location in the selection of University storage or processing facilities. Unless stated otherwise in this Agreement, this requirement does not apply to indirect or "overhead" services, redundant back-up services or services that are incidental to the performance of this Agreement. This provision applies to work performed by subcontractors at all tiers and to all University Data.

End of addendum, all else remains the same.