

REQUEST FOR PROPOSALS (RFP) NO. 25-2294  
TO  
PROVIDE A DIGITAL BADGING/MICRO-CREDENTIAL SOLUTION  
FOR  
UNIVERSITY OF HAWAII SYSTEM  
HONOLULU, HAWAII

SEPTEMBER, 2024

BOARD OF REGENTS  
UNIVERSITY OF HAWAII  
HONOLULU, HAWAII

## TABLE OF CONTENTS

RFP No. 25-2294 to Provide a Digital Badging/Micro-Credential Solution for the University of Hawai'i System, Honolulu, Hawai'i

	Pages
Notice to Offerors .....	1
Section 1. Administrative Overview .....	1-5
Section 2. Scope of Work .....	1-17
Section 3. Proposal Requirements .....	1-7
Section 4. Criteria to Evaluate Proposals .....	1-4
Section 5. Special Provisions .....	1-7
ATTACHMENT A .....	1
ATTACHMENT B .....	1
ATTACHMENT C .....	1
APPENDIX A .....	1
APPENDIX B .....	2
APPENDIX C .....	2
APPENDIX D .....	1
APPENDIX E .....	1
APPENDIX F .....	1
APPENDIX G .....	2
APPENDIX H .....	2
APPENDIX I .....	1
APPENDIX J .....	1

APPENDIX K .....	1
APPENDIX L .....	2
APPENDIX M .....	2

**IT IS THE RESPONSIBILITY OF ALL OFFERORS TO CHECK THE TABLE OF CONTENTS TO CONFIRM THAT ALL PAGES LISTED THEREIN ARE CONTAINED IN THEIR RFP PACKAGE.**

## NOTICE TO OFFERORS

The University of Hawaii RFP No. 25-2294, to Provide a Digital Badging/Micro-Credential Solution for the University of Hawai'i System, Honolulu, Hawai'i is issued and will be awarded through the State of Hawaii's electronic procurement system (HlePRO). **All proposal responses must be submitted electronically through HlePRO no later than 2:30 p.m., October 31, 2024** Proposal received after the due date and time or received in a form other than electronically through HlePRO will not be considered.

Offerors are advised that they should not wait until the last minute to submit their proposal through HlePRO. Offerors are solely responsible for ensuring that their electronic submission through HlePRO is complete and all necessary files are attached to their offeror prior to the RFP due date and time. The University shall not be responsible for any delay or failure of any Offeror to submit any materials updated through the RFP process on a timely basis.

### Electronic Procurement

Offerors interested in responding to this electronic solicitation must be registered on HlePRO. To register, visit the following link: [https://hiepro.ehawaii.gov/videos/video/vendor\\_registration.html](https://hiepro.ehawaii.gov/videos/video/vendor_registration.html). Reference the Vendor Quick Reference Guide for additional information at <https://hiepro.ehawaii.gov/static-resources/VendorQuickReferenceGuide.pdf>.

HlePRO will be the system of record for the issuance of the the RFP, to receive the proposal requirements, issue Amendments, and make award for the RFP. Amendments and other information and materials provided through HlePRO, may include additions or changes with respect to the due date and time.

Special instructions in HlePRO related to this solicitation are incorporated herein and made a part of this RFP through reference. Offerors shall review all special instructions located in HlePRO.

### Questions and Clarifications

All questions and requests for clarifications must be submitted electronically through HlePRO. Questions must be submitted by **October 11, 2024**. Responses will be posted on **October 18, 2024**.

The University may refuse to answer any questions received outside of HlePRO or after the Questions/Answers deadline.

Kalbert K. Young  
Chief Procurement Officer  
University of Hawaii

Posting Date: October 1, 2024

***Vendors are responsible for notifying the Procurement Specialist Scott Shimoda (e-mail: [scottmhs@hawaii.edu](mailto:scottmhs@hawaii.edu)) for accessibility concerns related to this RFP.***

NOTICE TO OFFERORS

## **SECTION 1 ADMINISTRATIVE OVERVIEW**

### **1.1 INTRODUCTION**

This Request for Proposals (RFP) is being issued by the University of Hawai'i to solicit proposals from Offerors who wish to be considered to Provide a Digital Badging/Micro-Credential Solution for the University of Hawai'i System, Honolulu, Hawai'i.

### **1.2 AUTHORITY**

This Request for Proposals (RFP) is issued under the provisions of the Hawaii Revised Statutes, Chapters 103 and 103D. All prospective Contractors are charged with presumptive knowledge of all requirements of the cited authorities. Submission of a valid executed proposal by any prospective Contractor shall constitute admission of such knowledge on the part of such prospective Contractor.

### **1.3 RFP ORGANIZATION**

This RFP is organized into the following sections:

Section 1, Administrative Overview -- Provides Offerors with general information on the objectives of this RFP, procurement schedule, and procurement overview.

Section 2, Scope of Work -- Provides Offerors with a general description of the tasks to be performed, delineates University and Contractor's responsibilities, and defines deliverables.

Section 3, Proposal Requirements -- Describes the required format and content for the Offeror's proposal.

Section 4, Criteria to Evaluate Proposals -- Describes how proposals will be evaluated by the University of Hawaii.

Section 5, Special Provisions -- Provides Offerors the terms and conditions under which the work will be performed.

1.4 SCHEDULE OF KEY DATES

The schedule of key dates set forth herein represents the University's best estimate of the schedule that will be followed. Any of the dates listed below may be changed at any time at the sole discretion of the Director, Office of Procurement Management:

RFP Advertised and Issued	<u>October 1, 2024</u>
Closing Date for Submission of Questions	<u>October 11, 2024</u>
University Response to Offeror's Questions	<u>October 18, 2024</u>
Closing Date for Receipt of Proposals	<u>October 31, 2024</u>
Proposal Review Period	<u>November 1 – 15, 2024</u>
Contractor Selection and Award	<u>November 20, 2024</u>
Contract Start Date (Tentative)	<u>January 1, 2025</u>

1.5 SUBMISSION OF QUESTIONS

Offerors may submit questions via HlePRO. The deadline for submission of questions is no later than 2:30 p.m., Hawaii Standard Time, on October 11, 2024.

Responses to question submitted via HlePRO will be made no later than 4:30 p.m., Hawaii Standard Time, on October 18, 2024

1.6 SUBMISSION OF PROPOSALS

Offerors shall read, complete, and submit all required information as specified in the Request for Proposals. All proposals must be submitted via HlePRO by the date and time specified on the NOTICE TO OFFERORS. No hardcopy proposals will be accepted.

1.7 COSTS FOR PROPOSAL PREPARATION

Any costs incurred by Offerors in preparing or submitting a proposal shall be the Offeror's sole responsibility.

## 1.8 DISQUALIFICATION OF PROPOSALS

The University reserves the right to consider as acceptable only those proposals submitted in accordance with all requirements set forth in this RFP and which demonstrate an understanding of the scope of the work. Any proposal offering any other set of terms and conditions contradictory to those included in this RFP may be disqualified without further notice.

An Offeror may be disqualified and the proposal may be automatically rejected for any one or more of the following reasons:

1. The proposal shows any noncompliance with applicable law.
2. The proposal is conditional, incomplete, or irregular in such a way as to make the proposal indefinite or ambiguous as to its meaning.
3. The proposal has any provision reserving the right to accept or reject award, or to enter into a contract pursuant to an award, or provisions contrary to those required in the solicitation.
4. The Offeror is debarred or suspended.

## 1.9 PROCUREMENT OFFICER

This RFP is issued by the Office of Procurement Management, University of Hawaii. The Procurement Officer responsible for overseeing the contract is Karlee Hisashima , Interim Director of the Office of Procurement Management.

## 1.10 TECHNICAL REPRESENTATIVE OF THE PROCUREMENT OFFICER (TRPO)

The individual listed below is the Technical Representative of the Procurement Officer (TRPO):

Gloria Niles  
Directly, Online Learning, Information Technology Services  
University of Hawai'i 2520 Correa Road, IT Center, 5<sup>th</sup> Floor  
Honolulu, Hawai'i 96822  
Telephone:(808) 956-3504  
Email: [gniles@hawaii.edu](mailto:gniles@hawaii.edu)

### 1.11 ISSUING OFFICER

The individual listed below is the issuing officer and the official contact for all communication regarding this RFP:

Scott Shimoda, Procurement Specialist  
Office of Procurement Management  
University of Hawai'i  
1400 Lower Campus Road, Room 15  
Honolulu, Hawai'i 96822  
Phone: 808-956-8674  
Email: scottmhs@hawaii.edu

### 1.12 CHANGES TO CONTRACTOR'S FEE

It is recognized that audit disallowances and other changes may require adjustments in the compensation due to the Contractor. In the event that future actions would either disallow or minimize the payments already made to the Contractor, the Contractor shall assist the University in defending the correctness of the claim for reimbursement. If the disallowance or adjustment is upheld, then the Contractor will participate in the payback to the extent the amount of the disallowance or adjustment contributed to the total fee received by the Contractor. Payment to the University shall be made within THIRTY (30) calendar days from which official notice is received by the Contractor from the University.

### 1.13 RFP AMENDMENTS

The University reserves the right to amend the RFP any time prior to the closing date for best and final offers.

### 1.14 AWARD ON INITIAL PROPOSALS

The University may award a contract on the basis of initial offers received, without discussions. Therefore, each initial offer should contain the Offeror's best terms.

### 1.15 AVAILABILITY OF FUNDS

Offerors are advised that the award of this contract is contingent upon availability of funds. If funds are not available, the University reserves the right not to make award of this contract.



1.16 NOTICE TO PROCEED

The University shall not be responsible for work done, even in good faith, prior to the University's Notice to Proceed unless specific provisions are made in the contract.

1.17 RFP SUBMITTALS BECOME PROPERTY OF THE UNIVERSITY

All proposals and other material submitted shall become the property of the University and may be returned only at the University's option.

## **SECTION 2 SCOPE OF WORK**

### **2.1 PURPOSE**

To obtain the services of a CONTRACTOR to provide a digital badging/micro-credential SOLUTION for the University of Hawai'i System (UH), which offers digital badge ISSUERS and EARNERS with a single account for activity at multiple campuses and units across the state. The selected system must be interoperable with other badging systems and national credential platforms (such as Credential Engine) and accommodate "stackable" pathways. The UNIVERSITY requires the digital badge/micro-credential to be 1 Ed Tech-certified for Open Badges v.2.1 or higher.

### **2.2 OBJECTIVES**

The UNIVERSITY seeks to accomplish the following objectives with a digital badging/micro-credential platform:

- A. Provide a badge display, hosting, and badge issuing platform that provides EARNERS with a single account for activity at multiple campuses and units across the UNIVERSITY that would continue post-graduation.
- B. Provide allowance for extensive metadata to document learning outcomes, assessments, and links to evidence associated with earning a micro-credential within a digital badge.
- C. Provides data analytics and generates reports that track badging activity and usage at the system, campus, and department levels.

### **2.3 BACKGROUND**

The University of Hawai'i (UH) is the state's public system of higher education. The University consists of TEN (10) separately accredited campuses located on the island of O'ahu, Kaua'i, Maui, and Hawai'i: UH Mānoa, UH Hilo, UH West O'ahu, Hawai'i Community College, Honolulu Community College, Kapi'olani Community College, Kaua'i Community College, Leeward Community College, UH Maui College and Windward Community College. Community-based Learning Centers support students in areas of the Hawaiian Islands that are geographically distanced from a University campus. The Learning Centers comprise THREE (3) systemwide University Centers that connect students to bachelor's and graduate degree programs and SIX (6) campus-sponsored Education Centers that support students in acquiring a degree or certificate, often through distance education programs.

The University of Hawai'i offers opportunity and hope for every resident of Hawai'i. As the sole provider of public higher education in the state, the University can drive a more vibrant, sustainable, resistant, just, and kind future across our islands. The University's scholarship must address the opportunities and challenges of Hawai'i, the Pacific, and our planet. The University of Hawai'i aspires to be grounded in traditional Hawaiian values, in aloha, to create a sense of place while also service as a forward-looking economic engine driving a hub of innovation and research.

As the University of Hawai'i begins its 118<sup>th</sup> year of service, it must remain vigilant, anticipate what is coming, and act with agility and compassion to maintain a vital role in shaping the future of its island home. It must be Hawai'i's University for today and tomorrow.

The 2023-2029 University of Hawai'i Strategic Plan: <https://www.hawaii.edu/offices/vp-academic-strategy/uh-strategic-plan-2023-2029/guiding-principles/> outlines the strategic imperatives of the University:

- Fulfill kuleana (responsibility) to Native Hawaiians and Hawai'i;
- Develop successful students for a better future;
- Meet Hawai'i's workforce needs for today and tomorrow;
- Diversify Hawai'i's economy through UH innovation and research.

The strategic imperative to “Meet Hawai'i's workforce needs for today and tomorrow” includes an objective to “Enhance non-traditional offerings, including micro-credentials serving the needs of specific groups of students and industry certified and non-credit credentials, for those seeking upskilling or career change opportunities.” Micro-credentials at UH are further defined under [Executive Policy 5.231](#).

Micro-credentials are a core strategy of the University of Hawai'i and continue to be elevated with digital badging. The RFP for a digital badging/micro-credential platform is critical component of UH's development of its micro-credentialing efforts.

## 2.4 DEFINITIONS

- A. **CONTRACT** – The written agreement between the parties, including but not limited to the Request for Proposal (“RFP”) and its specification, terms, and conditions; solicitation addenda and contract amendments, if any; and will be the resulting Contract for the digital badging/micro-credential platform.
- B. **CONTRACTOR** – The person or the Organization with whom the UNIVERSITY has contracted to provide services and receive rights pursuant to this CONTRACT.

- C. DATA – Information or data elements that are created, received, maintained, and/or transmitted by the UNIVERSITY in the course of meeting its administrative and academic requirements and include, without limitation, non-public information, student data, metadata, and user content. Data may fall into ONE (1) of FOUR (4) data classification categories, as outlined in the UNIVERSITY’s Executive Policy EP 2.214, Institutional Data Classification Categories and Information Security Guidelines: <https://www.hawaii.edu/policy/index.php?action=viewPolicy&policySection=ep&policyChapter=2&policyNumber=214&menuView=closed>.
- D. CISCO – Chief Information Security Officer.
- E. EARNER – The individual who achieves the criteria for a micro-credential and is issued a digital badge.
- F. FERPA – Family Educational Rights and Privacy Act of 1974.
- G. FTE – Full-Time Equivalent.
- H. ISSUER - The creator and distributor of digital badges for earned micro-credentials.
- I. OFFEROR – Any respondent to this RFP. The successful OFFEROR becomes the CONTRACTOR. Statements referring to the term “Offeror” generally indicate requirements by and respondent, which must be included in its proposal. Statements referring to “Contractor” generally indicate requirements that will become contractual obligations.
- J. PII – Personally Identifiable Information is any information identified as personally identifiable information under FERPA or applicable federal or state law.
- K. PROJECT MANAGER – The administrator overseeing the UNIVERSITY’s Digital Badging/Micro-credential Platform.
- L. PROPOSAL – The OFFEROR’S response to the RFP.
- M. RFP – The University of Hawai’i System requests for proposal 25-2294 to Provide a Digital Badging/Micro-credentials Platform for the University of Hawai’i System.
- N. SOLUTION – The OFFEROR’S proposed Digital Badging/Micro-credentials platform.
- O. UNIVERSITY/UH – The corporate entity known as the University of Hawai’i.

- P. VENDOR – A company contracted or subcontracted to provide services to the UNIVERSITY and/or to receive DATA from the UNIVERSITY, including all its officers, employees, agents, and representatives.

## 2.5 TECHNICAL AND DATA CAPABILITIES

The Digital Badging/Micro-credential system SOLUTION shall include the following technical and DATA features:

### A. Integrations

#### 1. Browser and Device Agnostic

- a. The SOLUTION must access any of the CONTRACTOR's applications using major, commercially available web browsers, such as Edge, Safari, Firefox, or Chrome.
- b. With no limitations, The SOLUTION must run natively and responsively on any mobile device, including smartphones, tablets, Chrome Books, laptop computers, and desktop computers.

#### 2. Mobile Application

- a. A mobile application must support the SOLUTION.
- b. The mobile application must be available for iOS and Android.
- c. The mobile application must be free of charge for users to access.

#### 3. Learning Management System

- a. The SOLUTION must integrate with the UNIVERSITY'S learning management system, Brightspace by D2L, for the transfer of DATA from and to the SOLUTION.

#### 4. Student Information System (SIS) Integration

- a. The SOLUTION must integrate with the UNIVERSITY'S non-credit Student Information System, Modern Campus, for user account creation and ongoing micro-credential management.
- b. The SOLUTION must integrate with the UNIVERSITY's Student Information System, Ellucian-Banner, for user account creation, badge issuing, and ongoing micro-credential management.

- c. The SOLUTION must support bulk import and export of DATA from and to the SOLUTION (e.g., editing groups and issuing digital badges).
- d. The SOLUTION must provide real-time or near real-time import and export of DATA from and to the SOLUTION.

#### 5. Single Sign On

- a. The SOLUTION must support the UNVIERSITY's SSO.

#### 6. Authentication Authorization

- a. The SOLUTION must support Multi-Factor Authentication (MFA) either core to the SOLUTION or via third-party application (e.g., DUO, DUO Mobile app, Yubikey hard token), specifically, Two-Factor Authentication (2FA), which allows access by requiring TWO (2) source methods to verify identity.

### B. Hosting Services

1. The SOLUTION must be cloud-hosted.
2. The SOLUTION must provide the capability to support central hosting for Campuses through Software as a Service (SaaS).
3. All of the UNIVERSITY'S DATA must be hosted in the United States of America.
4. The CONTRACTOR must provide storage capacity and storage management support.
5. The SOLUTION must have a backup and restore plan in case of a serious issue (i.e., server outage or server failure).
6. The SOLUTION must handle virus-infected (e.g., malware) files. The SOLUTION shall identify and quarantine or remediate virus-infected files when uploaded to the SOLUTION.
7. The SOLUTION must be able to retrieve all DATA stored in the system on behalf of the UNIVERSITY.

### C. System Administration

1. The SOLUTION must allow system administrators to develop an institutional hierarchy that supports ISSUERS across multiple campuses and departments as sub-accounts.

### D. Institutional Level Reporting and Statistics

1. The SOLUTION must provide a DATA interface to pull real-time DAT, including, but not limited to:
  - a. Track digital badges earned, claimed, shared, and published.
  - b. Analytics event log – accurate engagement tracking and reports for micro-credentials earned and digital badges issued.
  - c. Track the number of clicks to the issuer's website.
  - d. Social media analytics - accurately track digital badges added and viewed across social media platforms.

### E. Web Accessible Content

1. The OFFEROR must describe how the SOLUTION meets current industry standards (WCAG Level 2.1 AA) for accessibility, particularly regarding the web pages that display EARNERS' digital badges intended for public consumption.
2. The SOLUTION must support ADA compliance; Web Content Accessibility (WCAG Level 2.1 AA) compliant for digital badge issuing.

## 2.6 KEY FEATURES

The Digital Badging/Micro-Credentials system SOLUTION shall include the following features to meet the UNIVERSITY'S digital badging and micro-credential requirements.

### A. Badge Issuing, Display, and Housing

1. The SOLUTION must provide the ability to create and issue digital badges based on micro-credential criteria established by the UNIVERSITY.
2. The SOLUTION must display digital badges issued by the UNIVERSITY.

3. The SOLUTION must be able to host digital badges from ISSUERS outside of the UNIVERSITY and imported from other Open Badges-certified platforms.

#### B. Open Badges Standards

1. The UNIVERSITY requires the CONTRACTOR to be Open Badges v2.0 issuer, displayer, and host and be able to certify in OPEN Badges 3.0 within six (6) months of the contract date, or 1EdTech-certified as an OPEN Badges 3.0 issuer, displayer, and host.
2. 1EdTech certificated in the ability to move credentials via Open badges v2.1 Badge Connect API or have implemented the Open Badges 3.0 API.
3. The vendor is required to provide a valid and current 1EdTech certification registration number. See [1edtech.org](http://1edtech.org).
4. The CONTRACTOR is also required to remain current with subsequent versions of the Open Badges standard and receive certification within a 6-month time period.

#### C. Digital Badge Issuer User Interface

1. The SOLUTION must provide a user-friendly graphical user interface to create and issue badges.
2. The SOLUTION must provide for the ability to create pathways and alignment capabilities for stackable micro-credentials across multiple UH campuses and departments.

#### D. Digital Badge Branding

1. The SOLUTION must allow for customization of digital badges of ISSUERS and the digital badge display for EARNERS as needed (e.g., white labeling).
2. The SOLUTION must allow for customization and branding of digital badges and the digital badge issuing platform, aligning with the UNVIERSITY'S branding criteria.
3. The SOLUTION must allow ISSUERS to enable modifications, settings, and branding for each college and each badge.



## E. Metadata

1. The SOLUTION must contain a rich set of properties (metadata) about the achievement that validates the micro-credential, including, but not limited to:
  - a. Accreditation – An extension to include metadata about an issuing organization’s accrediting body.
  - b. Alignment – Metadata referencing alignment to an external framework (e.g. state education standards, skill or competency framework).
  - c. Assessment – An extension that provides a way to include metadata about how the criteria for a digital badge was assessed.
  - d. Criteria – Descriptive, formattable, metadata about the achievements necessary to earn a badge.
  - e. Endorsement – The ability for a third party to make supportive claims about a badge, issuing organization, or EARNER.
  - f. Evidence – Descriptive metadata about evidence related to the issuance of a badge.
  - g. Expiration – The ability to establish an expiration date on an issued badge.
  - h. Multilingual – The ability to issue a badge in multiple languages, including ‘Ōlelo Hawai‘i (Hawaiian language).
  - i. Revocation – The ability to revoke badges after they have been issued.
  - j. Versioning – The ability to issue updates of a badge without altering previously issued versions of the badge.

## F. Digital Badge EARNER Capabilities

1. The SOLUTION must allow the EARNER to download and store the digital badge locally or upload it to an Open Badges host of their choosing without losing the original badge data.
2. The OFFEROR must describe the method they use for EARNERS to display their digital badges.

3. The SOLUTION must provide the ability to ensure the EARNER owns and manages the digital badge.
4. The SOLUTION must provide the ability for the EARNER to share the digital badge via a unique URL that can be shared.
5. The SOLUTION must allow the EARNER to keep the digital badge private and secure by ensuring that EARNERS have agency about what to share, with whom to share, and where to share.
6. The SOLUTION must allow the EARNER to determine if a digital badge is public or private.

G. FERPA Compliance

1. The SOLUTION must provide support for FERPA compliance.

2.7 TRAINING AND SUPPORT

- A. The SOLUTION must provide training resources and support for digital badge ISSUERS.
- B. The SOLUTION must provide training resources and support for digital badge EARNERS.
- C. The SOLUTION must provide ongoing technical support for both ISSUERS and EARNERS.

2.8 DATA SHARING PROTECTIONS AND REQUIREMENTS

The Digital Badging / Micro-Credentials SOLUTION shall include the following features to meet the UNIVERSITY'S DATA sharing protections and requirements:

- A. Ownership of DATA  
The UNIVERSITY shall maintain ownership of the DATA, and all proprietary rights to the DATA, including intellectual property rights, shall be and remain in the UNIVERSITY.

B. Transmission of DATA

All DATA transmitted shall be by secure means and shall be encrypted.

### C. No Warranties

The UNIVERSITY makes no representation or warranties of any kind or nature, express or implied, regarding the DATA, including, without limitation, its quality or fitness for any particular purpose. In no event shall the UNIVERSITY be liable for VENDORS's use of the DATA as set forth herein.

### D. DATA Confidentiality

VENDOR shall treat the DATA as confidential and shall implement appropriate measures designed to ensure the confidentiality of the DATA, including, without limitation, restricting access to only personnel who require such access and the use of such DATA to perform the activities permitted and required personnel with access to the DATA to sign written confidentiality agreements.

### E. Network Security

VENDOR shall maintain network security sufficient to protect the DATA and in conformance with generally recognized industry standards and best practices, including, without limitation: (a) network firewall provisioning; (b) maintaining patched environments with appropriate security updates; (c) intrusion detection; (d) annual third-party risk assessments; and (e) regular vulnerability scans.

### F. Application Security

VENDOR shall maintain and regularly update its software such that applications remain secure from vulnerabilities identified in updates, upgrades, and bug fixes.

### G. DATA Security

VENDOR shall implement measures to secure the DATA including, without limitation; (a) ensuring the transmission and storage of DATA by secure means, including encryption of all DATA; (b) maintaining the DATA on designated secure servers and/or secure endpoint computers; (c) prohibiting the storage of DATA on portable or laptop computing devices, or portable storage devices or similar mediums unless that medium is used as part of a backup and recovery process; (d) requiring the storage, backup, and network paths utilized for the DATA be contained within the United States; (e) adopting policies to secure the DATA from unauthorized access and to address breaches; (f) transmitting, storing and processing the DATA in accordance with industry best practices; and (g) conducting annual risk assessments.

#### H. Disclosure to Third Parties Prohibited

VENDOR shall not reveal, transmit, exchange, or share the DATA with subcontractors or other third parties unless VENDOR has obtained the UNIVERSITY'S prior written consent, provided that if VENDOR obtains the UNIVERSITY'S prior written consent, VENDOR shall enter into a written agreement with subcontractor or other such third parties ("Permitted Subcontractors") that require and ensure that each such Permitted Subcontractor (a) maintains at least the same level of DATA protection, security, confidentiality, and indemnification as is required of VENDOR hereunder with respect to the DATA, VENDOR shall be responsible for its Permitted Subcontractor' use of the DATA hereunder.

#### I. Destruction of DATA

Upon termination of this CONTRACT, written request from the UNIVERSITY, or cessation of any need for the DATA, whichever occurs first, VENDOR shall erase, destroy, and render unreadable all DATA provided to VENDOR under this CONTRACT in a manner that prevents reconstruction or re-identification of such DATA. Within thirty (30) days of a request from the UNIVERSITY, VENDOR shall provide written certification that these actions to erase, destroy, and render unreadable all DATA have been complied with.

#### J. Compliance with Applicable Laws

VENDOR shall observe and comply with all applicable laws, statues, ordinances, orders, directives, rules, and regulations, now or hereafter, made by any governmental authority (" Applicable Laws") regarding DATA security and protections.

#### K. Compliance with Applicable UNIVERSITY Policies

VENDOR shall observe and comply with all applicable UNIVERSITY policies, including, without limitation,

1. Executive Policy EP 2.214, Institutional Data Classification Categories and Information Security Guidelines:  
<https://www.hawaii.edu/policy/index.php?action=viewPolicy&policySection=ep&policyChapter=2&policyNumber=214&menuView=closed>.
2. Executive Policy EP 2.215, Institutional Data Governance:  
<https://www.hawaii.edu/policy/index.php?action=viewPolicy&policySection=ep&policyChapter=2&policyNumber=215&menuView=closed>.

3. Executive Policy EP 2.219, Student Online Data Protection Requirements for Third Party Vendors:  
<https://www.hawaii.edu/policy/index.php?action=viewPolicy&policySection=ep&policyChapter=2&policyNumber=219&menuView=closed>.
4. Administrative Procedure AP 7.022, Procedures Relating to Protection of the Educational Rights and Privacy of Students:  
<https://www.hawaii.edu/policy/index.php?action=viewPolicy&policySection=ap&policyChapter=7&policyNumber=022&menuView=closed>.

L. DATA Breach

VENDOR shall comply with all Applicable Laws, including, without limitation, Hawai'i Revised Statutes 487N, regarding notification in the event of the unauthorized release of PII or DATA, or other event requiring notification. Upon the confirmation of such event, VENDOR shall (a) notify the UNIVERSITY by telephone or email within TWO (2) business days of confirmation, (b) assume financial responsibility and liability for the unauthorized disclosure, release, exposure, and/or breach, and (c) fully indemnify, defend, and hold harmless the UNIVRSITY, as further set forth herein. VENDOR shall pay all such associated costs necessary to address and provide relief of and from the adverse effects of such actual, probable, or suspected breach, exposure, or release of the DATA, including, without limitation, the costs of notifying all affected individuals and entities and making credit monitoring and restoration services available to such affected individuals and entities, as required by the UNIVERSITY and/or Applicable Laws.

#### M. Indemnification

VENDOR shall indemnify, defend with counsel reasonably acceptable to the UNIVERSITY, and hold harmless the UNIVERSITY, its officers, employees, agents, representatives, and any person acting on its behalf from and against any and all claims, demands, suits, actions, causes or action, judgements, injunctions, orders, rulings, directives, penalties, assessments, liabilities, losses, damages, costs, and expenses (including, without limitation, reasonable attorneys' fees, expert witness fees and costs, discover and pretrial costs, and costs incurred in the investigation, prosecution, defense, and/or handling of any action) by whomsoever incurred, sustained, or asserted, including claims for property damage, personal injury, death, lost revenues, and other economic loss and/or environmental damage, directly or indirectly arising or related in any way to : (a) the sharing or making available of the DATA hereunder; (b) VENDORS use, handling, transmission storage, processing of any DATA; (c) VENDOR's unauthorized use, handling, transmission storage, processing, disclosure, release, and/or exposure of DATA; and/or (d) VENDOR's failure to timely, fully and properly perform any of its obligations under this CONTRACT, particularly any obligation relating to DATA sharing and protection.

#### N. Mandatory Disclosure of PII

In the event VENDOR becomes compelled by law or government directive to disclose any PII, VENDOR shall provide the UNIVERSITY with immediate written notice so that the UNIVERSITY may seek an appropriate protective order or other remedy. VENDOR shall only furnish that portion of the PII necessary to comply with the law or directive.

#### O. Injunctive Relief

Violation of any terms herein, including the actual or potential disclosure, release, and/or exposure of DATA, may cause the UNIVERSITY irreparable injury for which there is no adequate remedy at law, and consequently, the UNIVERSITY is entitled to seek immediate injunctive relief prohibiting such violation, in addition to any other rights available to it. VENDOR hereby waives any requirement to post a bond with respect to any action for injunctive relief.

## P. Survival

All VENDOR's obligations herein to protect and secure DATA, as well as to assume financial responsibility and liability for any unauthorized use, handling, transmission, storage, processing, disclosure, release, and/or exposure of DATA and to indemnify, defend, and hold harmless the UNIVERSITY hereunder, shall survive termination or expiration of this CONTRACT.

## 2.9 IMPLEMENTATION

A. Implementation of the SOLUTION shall follow the estimated timeline:

1. November – December 2024 – Administrative planning for system configuration and testing integrations and training for digital badge ISSUERS.
2. January- February 2025 – Training shall be provided for digital badge EARNERS.
3. March 2025 – Complete SOLUTION implementation for issuing, displaying, and hosting digital badges.

The implementation timeline is an estimate and is subject to change.

B. System Configuration and Testing Integrations

1. The CONTRACTOR shall provide technical assistance with managing system configuration, branding, and establishing integrations with the hosting service provider.
2. The CONTRACTOR shall provide technical assistance with system configuration, the organizational hierarchy of the SOLUTION, and its development.
3. The CONTRACTOR shall support testing the integration with the UNIVERSITY'S Student Information System, multi-factor authentication system, and any third-party API and Learning Tools Interoperability (LTI) integrations.

C. Partnership

1. The CONTRACTOR shall provide technical assistance, documentation, and resources to support stakeholder engagement throughout implementation.

2. The CONTRACTOR shall provide resources for the ongoing partnership with the UNIVERSITY throughout the contract term to respond to feedback and address technical and functional questions and concerns related to the SOLUTION, support, and product enhancements
3. The CONTRACTOR shall provide resources for ongoing technical support to ISSUERS and Information Technology Services Help Desk managers.

D. Training

1. The UNIVERSITY PROJECT MANAGER, in consultation with a client services manager assigned by the CONTRACTOR, shall coordinate training activities centrally.
2. The CONTRACTOR shall provide online training (e.g., webinars) for the orientation and formal end-user training. The UNIVERSITY shall receive a recording of live webinars for on-demand playback at a later date by users.
3. Training shall be provided in groups by unit, campus, or various other campus-based groups determined by the CONTRACTOR in consultation with the UNVIERSITY.
4. During implementation, the CONTRACTOR shall provide in-depth, remote training for the UNIVERSITY'S Information Technology Services staff managing ISSUERS, the UNIVERSITY'S Help Desk support staff.
5. The CONTRACTOR shall provide on-demand resources to support initial and ongoing training for faculty and instructional designers on developing micro-credential pathways, metadata and issuing digital badges.
6. The CONTRACTOR shall provide access to training resources to introduce ISSUERS and EARNERS to the full scope of issuing, displaying, and hosting features of the SOLUTION through on-demand videos and online content throughout the term of the CONTRACT.



## 2.10 MINIMUM QUALIFICATIONS OF OFFEROR

The intent of this RFP is to provide a digital badging/micro-credential platform solution for the UNIVERSITY that provides EARNERS with a single account for activity at multiple campuses and units. The UNIVERSITY believes that the OFFEROR's Cybersecurity and Disaster Recovery Plans, Standards-Based Compliance, and Accessibility are important in assessing the OFFEROR's potential to meet the UNIVERSITY'S purpose and objectives. Accordingly, the prospective OFFEROR must conform to the following minimum qualifications and provide the required information in order to be considered for award. OFFEROR shall complete Appendix G, Offeror Minimum Qualification Matrix, to establish that all minimum qualifications have been met.

### A. Have both Cybersecurity and Disaster Recovery Plans.

#### 1. Provide the following documents:

- a. SOC 2 certification (the UNIVERSITY'S CISO can sign a Non-Disclosure Agreement)
- b. Privacy statement, including FERPA compliance
- c. Security plan and practices
- d. DATA flow diagram
- e. Network architecture diagram
- f. Disaster recovery plan

### B. Have Standards-Based Compliance

1. Indicate that the following certifications are verifiable through 1EdTech (available at [1edtech.org](http://1edtech.org)) or submit an alternative certification with a detailed explanation of how the alternative certification is comparable to the certification through 1EdTech.
  - a. Open Badges v.2.0 or v.3.0 Type: issuer, Displayer, Host
  - b. Open Badges v.2.1 or v.3.0 API Support Service Provider

### C. Demonstrate Accessibility

1. Submit an Accessibility Conformance Report completed utilizing Voluntary Product Accessibility Template VPAT 2.3 and Web Content Accessibility Guidelines (WCAG 2.1). The accessibility evaluation submitted must correspond to the current version of the proposed SOLUTION.
2. Submit a comprehensive accessibility evaluation from an objective, independent third party verifying the claims made on the product Accessibility Conformance Report (VPAT 2.3), or equivalent, if an independent third party did not complete the Accessibility Conformance Report. OFFEROR may use a third-party accessibility evaluation service of their choice.

## **PROPOSAL REQUIREMENTS**

### **3.1 INTRODUCTION**

This section indicates the proposal requirements for this RFP which shall be submitted by the deadline set for submission of proposals. Fulfillment of all proposal requirements listed is mandatory for consideration of proposals.

The Proposal shall include the following subsections:

Proposal Letter

Business Classification Certification Statement

Price Quotation Sheet

Executive Summary

Company History and Organization

Product Roadmap

Offeror Minimum Qualification Matrix

Technical and Data Capabilities

Key Features

Training and Support

Data Sharing Protections and Requirement Capabilities

Implementation Plan

References

Offeror's proposals should include each of the appendices and be placed in the order provided in sections 3.2 through 3.14. To assist the Offeror, a checklist and Appendices A through M are provided as a separate document.

### **3.2 PROPOSAL LETTER (Appendix A)**

The Proposal Letter shown in Appendix A shall be signed by an individual authorized to legally bind the Offeror, dated, and be affixed with the corporate seal (if corporate seal is available). If said individual is not the corporate president, evidence shall be submitted showing the individual's authority to bind the corporation. The fully executed proposal letter shall be submitted along with the proposal.

### 3.3 BUSINESS CLASSIFICATION CERTIFICATION STATEMENT (Appendix B)

OFFERORS shall complete and submit the Business Classification Certification Statement document with the proposal.

### 3.4 PRICE QUOTATION SHEET (Appendix C)

Offeror shall provide a price quotation for the digital badging/micro-credentials solution on the information provided in Appendices D through K, which shall include the following:

- A. Licensing fees are based on the user type and number of users. Refer to ATTACHMENTS A, B and C to determine the number of licenses based on Headcount Enrollment, Faculty Count, and Employee FTE. Licensing fees shall commence upon satisfactory implementation and acceptance of the digital badging/micro-credentials platform and shall be projected out for a FIVE (5) year term in accordance with the estimated implementation timeline in Section 2.9 and thereafter paid on a fixed, annual basis.
- B. One (1)- time fees for implementation services (e.g., Configuration and Testing Integrations, Partnership, Training and Support) that the Offeror is providing to the University. One (1) – time fees shall be assessed to the University in accordance with the estimated implementation timeline in Section 2.9.
- C. All fees shall include hardware, software, maintenance, mobile application costs, man-hours, travel-related expenses, overhead, and all applicable fees and taxes.

Complete Appendix C, Price Quotation Sheet. All rows in the worksheet must be completed. If no costs are associated with any item, an "N/A" designation shall be indicated, and the Offeror is not to assess any cost for that line item.

### 3.5 EXECUTIVE SUMMARY (APPENDIX D)

- A. Offeror shall provide an Executive Summary that includes a brief overview of Offeror's proposal summarizing the anticipated results, as well as an overview of the process that the Offeror intends to follow to achieve these results.

### 3.6 COMPANY HISTORY AND ORGANIZATION (APPENDIX E)

A. Offeror shall provide information regarding Offeror's company history and organization in the following areas:

1. Company headquarters information.
2. Company ownership structure.
3. Number of years in business.
4. Awards and merits.
5. Software evolution and direction.
6. Evidence of financial stability.
7. Previous experience implementing projects similar in scope.

### 3.7 PRODUCT ROADMAP (APPENDIX F)

A. Offeror shall provide their plan for future updates to the solution as they relate to the following questions:

1. Describe how items are prioritized on the product roadmap.
2. How often is the product roadmap updated?
3. How often is the product roadmap made publicly available and/or available to partnering institutions.

### 3.8 OFFEROR MINIMUM QUALIFICATIONS (APPENDIX G)

The Offeror Minimum Qualification Matrix shown in Appendix G and referred to in Section 2.10 shall be submitted together with all of the required documents and information to establish that all minimum qualifications have been met.

### 3.9 TECHNICAL AND DATA CAPABILITIES (APPENDIX H)

Offeror shall provide details on how their solution meets the technical and data requirements of the University as referred to in Section 2.5, and shall also address specific issues as follows:

A. Integrations

1. Browser and device agnostic
  - a. Describe how the solution functions across various web browsers.

2. Describe how the solution runs natively and responsively across various device types (e.g., desktop, laptop, tablet, smartphone).
3. Mobile Application
  - a. Describe the availability of a mobile application for the solution.
  - b. Describe any limitations or differences in functionality for digital badge display and sharing between the website and the mobile application.
4. Learning management System Integration
  - a. Describe in detail the integration capabilities between the solution and Brightspace learning management system.
5. Student Information System (SIS) Integration
  - a. Describe how the solution integrates with the University's Non-Credit Student Information System, Modern Campus.
  - b. Describe how the solution integrates with the University's Student Information System, Ellucian-Banner.
6. Single Sign On (SSO)
  - a. Describe how the solution supports the University's SSO.
7. Authentication Authorization
  - a. Describe how the solution supports Two-Factor MFA.

## B. Hosting Services

1. Indicate where the application is hosted and where the data is hosted.
2. Describe where the data is hosted.
3. Describe the server response time, uptime guarantees, and maintenance schedule.
4. Describe the storage capacity and storage management support.
5. Describe how the solution will handle virus-infected (e.g., malware) files.

Describe how virus-infected files will be identified and quarantined or remediated when uploaded to the solution.

6. List and describe any security breaches and incidents compromising confidential information during the last FIVE (5) years.

#### C. System Administration

1. Indicate any content or solution areas that are restricted system administrator access.

#### D. Institutional Level Reporting and Statistics

1. Describe in detail the types of reporting and analytic capabilities of the solution.

#### E. Web Accessible Content

1. Describe in detail the solution's web accessible content features.

### 3.10 KEY FEATURES (APPENDIX I)

Offeror shall provide details on how their solution meets the key feature requirements of the University as referred to in Section 2.6, summarized as follows:

- A. Badge Hosting and Issuing
- B. Open Badges Standards
- C. Digital badge Issuer User Interface
- D. Metadata
- E. Digital Badge Earner Capabilities
- F. FERPA Compliance

### 3.11 TRAINING AND SUPPORT (APPENDIX J)

Offeror shall provide details on training and support provided for the solution as referred to in Section 2.7, summarized as follows:

- A. Describe training and support provided for badge issuers.
- B. Describe training and support provided for badge earners.

C. Describe ongoing technical support for badge issuers and badge earners.

### 3.12 DATA SHARING PROTECTIONS AND REQUIREMENT CAPABILITIES (APPNEDIX K)

Offeror shall provide a data sharing protection plan that provides details on how their solution meets the data sharing protections and requirements of the University as referred to in Section 2.8, and shall also address specific issues as follows:

- A. Describe the transmission of data and network security based on the data flow diagram and network architecture diagram referenced in Section 2.8 and Appendix G.
- B. Describe the Offeror's data confidentiality policies.
- C. Describe the Offeror's application security such as software update, upgrades, and patch schedules.
- D. Describe how the Offeror will fulfill the elements described in Section 2.8, Sub-item G, Data Security.
- E. Describe the Offeror's policy and/or procedures around disclosure to third parties.
- F. Describe the Offeror's policies and/or procedures around destruction of data.
- G. Describe the Offeror's policies and/or procedures around data breaches and mandatory disclosures of PII, as evidenced by incident response and data breach procedures.

### 3.13 IMPLEMENTATION OF PLAN (APPENDIX L)

Offeror shall provide a detailed implementation plan based on the estimated implementation timeline in Section 2.9, which shall also address specific issues as follows:

- A. Describe the technical assistance provided with managing system configuration, branding, and establishing integrations with the hosting service provider.
- B. Describe the technical assistance provided with the solution's system configuration and organizational hierarchy.
- C. Describe the support provided for testing the integration with the University's



Student Information System, multi-factor authentication system.

- D. Describe the technical assistance, documentation, and resources to support stake holder engagement.
- E. Describe the resources provided for an ongoing partnership with the University throughout the term of the contract to respond to feedback and address technical and functional questions and concerns related to the solution, support, and product enhancements.
- F. Describe the resources provided for ongoing technical support to digital badge issuers and Information Technology Services Help Desk managers.
- G. Offeror must complete the table in Appendix L, outlining the tasks involved with the implementation of the solution as referenced to in Section 2.9, including the start and end dates of each task, description of the resources required and/or provided, and the responsible party for each task.

#### 3.14 REFERENCES (APPENDIX M)

Offeror shall provide THREE (3) references of institution comparable to the University in enrollment, cost, and the use of a digital badging platform for issuing, displaying, and hosting of digital badges. The Offeror is highly encouraged to select references whose institution utilizes Brightspace by D2L as their LMS and uses the solution to create stackable pathways for micro-credentials. The name of the institutions, addresses, contact persons and positions, phone numbers, email address, full-time equivalent of the institutions, and the use of the digital badging/micro-credential platform for issuing, displaying, and hosting digital badges shall be furnished.

The University shall contact the references to determine the Offeror's expertise and knowledge in implementing a digital badge/micro-credential platform for institutions of similar size.

## **SECTION 4 CRITERIA TO EVALUATE PROPOSALS**

The evaluation of proposals received in response to the RFP will be conducted comprehensively, fairly, and impartially. Contracts will be awarded to responsive, responsible Offerors whose proposals are determined in writing to be the most advantageous to the University taking into consideration the evaluation factors set forth in this RFP.

A committee will evaluate and score each proposal submitted based on the following criteria:

- 4.1 The Offeror provides an Executive Summary, Company History, Organizational Information, and Product Roadmap, which will be evaluated as follows:  
**(30 points Maximum)**

- A. Executive Summary (10 points maximum)
- B. Company History (5 points maximum)
- C. Organizational Information (5 points maximum)
- D. Product Roadmap (10 points maximum)

- 4.2 Provides evidence that the Offeror meets all Cybersecurity and Disaster Recovery Plans, Standards-Based Compliance, and Accessibility requirement.  
**(70 Points Maximum)**

Offeror shall meet all requirements to receive the maximum points. If any of the qualifications or documents for Cybersecurity and Disaster Recovery Plans and Accessibility are omitted or determined by the CISO to be unacceptable, then the Offeror shall receive zero (0) points. If any of the Standards-Based Compliance certifications are not verifiable or an alternative certification comparable to the certification through 1EdTech is not provided, then the Offeror shall receive zero (0) points.

- 4.3 Provides evidence that the Offeror meets the University's Technical and Data Requirements. **(100 points maximum)**

Offeror shall meet all Technical and Data Requirements to receive the maximum points. If the Offeror does not meet a requirement, then the Offeror shall receive zero (0) points.

- 4.4 Provides evidence that the Offeror meets the University's Key Features Requirements, which will be evaluated as follows:  
**(250 points maximum)**

- A. Badge Issuing, Display and Hosting (60 points maximum)

- B. Open Badges standards (20 points maximum)
  - C. Digital badge Issuer User Interface (40 points maximum)
  - D. Digital Badge Branding (40 points maximum)
  - E. Metadata (40 points maximum)
  - F. Earner Capabilities (40 points maximum)
  - G. FERPA Compliance (10 points maximum)
- 4.5 Provide evidence that the Offer meets the University's Training and Support requirements, which will be evaluated as follow:  
**(50 points maximum)**
- A. Training and support provided for digital badge issuers (15 points)
  - B. Training and support provided for digital badge earners (15 points)
  - C. Ongoing technical support provided for digital badge issuers and earners (20 points)
- 4.6 Provide evidence that the Offeror meets the University's Data Sharing Protections and Requirements, which will be evaluated as follows:  
**(100 points maximum)**
- A. Transmission of Data and Network Security (Data flow diagram and network architecture diagram)
  - B. Data Confidentiality
  - C. Application Security
  - D. Data Security
  - E. Disclosure to Third Parties (as evidenced by policies and/or procedures)
  - F. Destruction of Data
  - G. Data Breach and mandatory Disclosure of PII (as evidenced by incident response and data breach procedures).

Offeror shall meet all Data Sharing Protections and Requirements to receive the maximum points. If the Offeror does not meet a requirement, then the Offeror shall receive zero (0) points.

- 4.7 The offeror has an implementation plan for its solution with a transparent methodology that meets the requirements for system configuration and testing integrations, partnership, and training, ensuring a smooth course and providing evidence of the strength of an ongoing collaboration between the Offeror and the University through implementation and throughout the term of the contract, which will be evaluated as follows:  
**(100 points maximum)**

A. System Configuration and Testing Integrations (50 points maximum)

B. Partnership (50 points maximum)

- 4.8 The Offeror demonstrates expertise and knowledge in implementing a digital badging/micro-credential platform for a multi-campus university system to institutions of similar size, including the migration/conversion of courses and content from legacy systems, which will be evaluated as follows:  
**(100 points maximum)**

Each reference may receive a maximum of 100 points. The total score of all three (3) references shall be divided by three (3) to determine the final points of the Offeror receives. Each reference will be evaluated as follows:

A. Similarity of institution in FTE and cost (10 points maximum)

B. Received digital badging issuing, displaying, and hosting services (10 points maximum)

C. Currently uses Brightspace by D2L as their enterprise learning management system (10 points maximum)

D. The institution offers digital badges for credit-bearing and not-credit micro-credentials in stackable pathways. (10 points)

E. Questions regarding implementation (20 points maximum)

F. Satisfaction with the product (20 points maximum)

G. Satisfaction with service (20 points maximum)

**4.9 Digital Badging/Micro-Credentials Platform Cost (200 points maximum)**

Overall, a maximum of TWO HUNDRED (200) points of the total evaluation points will be assigned to evaluate cost. In converting cost to points, the lowest cost proposal will automatically receive the maximum number of points allocated to the Digital badging/Micro-Credentials platform cost, 200 points. The point allocations for cost on the other proposals will be determined through the method set forth as follows:

$$[\text{Lowest Cost Proposal} \times 200 \text{ points (max.)}] / [\text{Offeror Proposal Cost}] = \text{Points}$$

Example:

Offeror A's Total Price; \$5,000 (Lowest Price) – Awarded 200 Points (maximum points)

Offeror B's Total Price: \$6,000 (Higher Price) – Awarded 166.67 Points (see calculation)

Offeror C's Total Price: \$7,000 (Highest Price) – Awarded 142.86 Points (see calculation)

Calculation:

Since Offeror A offers the lowest price, Offeror A receives the 200-point maximum. For Offerors B and C, the awarded points would be calculated as:

$$\text{Offeror B: } 200 \times \$5,000 / \$6,000 = 166.67$$

$$\text{Offeror C: } 200 \times \$5,000 / \$7,000 = 142.86$$

**TOTAL POSSIBLE POINTS; 1,000 Points**

## **SECTION 5 SPECIAL PROVISIONS**

### **5.1 SCOPE**

The Providing of a Digital Badge/Micro-Credentials Solution shall be in accordance with the terms and conditions of RFP No. 25-2294 and the General Provisions dated September, 2013 included by reference. Copies of the General Provisions are available at the Office of Procurement Management, University of Hawaii, 1400 Lower Campus Road, Room 15, Honolulu, Hawaii 96822 or the General Provisions may be viewed at: <https://www.hawaii.edu/procurement/vendor-info/terms-and-conditions/general-provisions-for-goods-and-services/>

### **5.2 TECHNICAL REPRESENTATIVE OF THE PROCUREMENT OFFICER (TRPO)**

The Technical Representative of the Procurement Officer is Scott Shimoda, (808) 956-8674.

### **5.4 REFERENCES**

The UNIVERSITY shall contact the references named in Appendix M, REFERENCES.

### **5.5 OPENING OF PROPOSALS**

Proposals will be opened at the date and time specified in Subsection 1.4, SCHEDULE OF KEY DATES, or as amended, at the proposal submittal office. The proposal opening will not be open to the public. Proposals may be available for public inspection upon notice of award and shall be available for public inspection after the contract is signed by all parties.

### **5.6 BEST AND FINAL OFFERS**

Priority-listed offerors may be afforded the opportunity to submit best and final offers as determined by the University. If the University requests best and final offers, and the priority-listed offerors do not submit a new offer, their immediate previous offer shall be considered as their best and final offer. If best and final offers are requested, and after best and final offers are received, final evaluations will be conducted by the University for purposes of award of the contract.

### **5.7 CONTRACT INVALIDATION**

If any provision of this contract is found to be invalid, such invalidation will not be construed to invalidate the entire contract.

## 5.8 RIGHTS AND REMEDIES OF THE UNIVERSITY FOR DEFAULT

In the event any service furnished by the CONTRACTOR in the performance of the CONTRACT should fail to conform to the specifications, the UNIVERSITY may reject the same, and it shall thereupon become the duty of the CONTRACTOR to correct same to conform to specifications, without expense to the UNIVERSITY provided that should the CONTRACTOR fail, neglect, or refuse to do so, the UNIVERSITY shall thereupon have the right to purchase in the open market, for the performance of such service and to deduct from any monies due or that may thereafter become due the CONTRACTOR, the difference between the price named in the CONTRACT and the actual cost thereof to the UNIVERSITY. In case any money due the CONTRACTOR is insufficient for said purpose, the CONTRACTOR shall pay the difference upon demand by the UNIVERSITY.

## 5.9 TERM

- A. The CONTRACT shall commence from the date designated in the Notice to Proceed with implementation and satisfactory operation of the Digital Badge/Micro-credentials Platform completed no later than March 2025.
- B. The initial term of the CONTRACT for Digital Badge/Micro credentials Platform shall be for a total of FIVE (5) years, and shall commence upon satisfactory implementation and acceptance of the Platform. Thereafter, the CONTRACT may be renewable from year to year for up to FIVE (5) additional years without the necessity of rebidding, upon mutual agreement in writing, NINETY (90) days prior to the renewal date.

## 5.10 INDEPENDENT CONTRACTOR

In the performance of services required under this Agreement, the CONTRACTOR is an "independent CONTRACTOR", with the authority and responsibility to control and direct the performance and details of the work and services required under the CONTRACT; however, the UNIVERSITY shall have a general right to inspect work to determine whether, in the UNIVERSITY'S opinion, the services are being performed by the CONTRACTOR in compliance with the CONTRACT. The CONTRACTOR and CONTRACTOR'S employees and agents are not by reason of this CONTRACT, agents or employees of the UNIVERSITY for any purpose, and the CONTRACTOR and the CONTRACTOR'S employees and agents shall not be entitled to claim or receive for the UNIVERSITY any vacation, sick leave, retirement, worker's compensation, unemployment insurance, or other benefits provided to UNIVERSITY employees. Furthermore, the CONTRACTOR intentionally, voluntarily, and knowingly assumes the sole and entire liability to the CONTRACTOR'S employees and agents in the course of their employment, and to any individual not a party to the CONTRACT, for all loss, damage, or injury caused by the CONTRACTOR, or the CONTRACTOR'S employees or agents in the course of their employment. The CONTRACTOR is

responsible for securing all employee-related insurance coverage for the CONTRACTOR and the CONTRACTOR'S employees and agents that is or may be required by law, and for payment of all premiums, cost, and other liabilities associated with securing the insurance coverage.

## 5.11 INSURANCE

Contractor shall, and shall ensure that all Contractor Agents shall, during the entire term of the contract, at no cost to University, procure and maintain, or cause to be procured and maintained, the following insurance described below, issued by an insurance company or companies authorized to do business in the State of Hawai'i with at least an A – VII Financial Rating according to the current edition of Best's Key Rating Guide:

### A. Required Insurance Coverage.

- (1) Commercial General Liability Insurance. Commercial general liability insurance written on occurrence basis covering claims with respect to injuries or damages to persons or property sustained as a result of the activities of the Contractor and/or the Contractor Agents within, on, or about the Premises and/or the University Campus, with limits not less than the following:

Bodily Injury and Property Damage Combined Single Limit	
\$1,000,000.00 Each occurrence	
\$2,000,000.00 General Aggregate per policy year	
\$2,000,000.00 Products and Completed Operations Aggregate per policy year	
Personal/Advertising Injury – Each occurrence	\$1,000,000.00
Medical Expenses -- Any one person	\$5,000.00
Damage to Rented Premises – Each occurrence	\$250,000.00

Personal/Advertising Injury coverage shall include coverage for mental injury, sexual harassment, sexual molestation or misconduct, invasion of privacy, and wrongful detention.

Such limits may be achieved through the use of umbrella/excess liability insurance sufficient to meet the requirements of this section 5.11 (Insurance) covering the Contractor's conduct of the services on or within the Premises and/or the University Campus and all of the activities and operations of the Contractor and the Contractor Agents in connection therewith.

- (2) Automobile Insurance. Automobile Liability Insurance to include coverage for any owned, non-owned, leased, or hired automobiles with limits of not less than the following:



Bodily Injury – Per Person	\$1,000,000.00
Bodily Injury – Per Accident	\$1,000,000.00
Property Damage – Each Accident	\$1,000,000.00
Basic No-Fault Insurance	As required by Hawai'i law

In the event there is a change in Hawai'i law regarding financial responsibility and insurance requirements of automobile owners or users which make this requirement obsolete, University shall have the right to impose a new requirement consistent with the then Applicable Laws.

(3) Workers' Compensation Insurance. Workers' Compensation insurance with respect to work by employees of the Contractor and the Contractor Agents on or about the Premises and/or the University Campus, with coverage, amounts, and limits as required by law.

(4) Employers Liability Insurance: Employers Liability Insurance with limits not less than:

Bodily Injury – Each Accident	\$1,000,000.00
Bodily Injury by Disease – Policy Limit	\$1,000,000.00
Bodily Injury by Disease – Each Employee	\$1,000,000.00

The Contractor shall ensure that the Contractor Agents (if any) obtain workers compensation and employer's liability insurance with the limits described herein to cover the work performed.

(5) Pollution Liability Insurance. If required by University in the event Hazardous Materials (as defined herein) are or may be involved or used, Pollution Liability insurance coverage with a combined single limit coverage of at least \$1,000,000 per occurrence which shall cover environmental liabilities, including, without limitation, claims for bodily injury, property damage, environmental damage, and remediation costs resulting from pollution conditions caused by the Contractor or the Contractor Agents and/or the conduct of the services.

B. Common provisions. Each insurance policy that Contractor and/or any of the Contractor Agents are obligated to obtain under the Contract shall be subject to the following:

(1) Notice of changes. Contractor will be required to notify University of any cancellation, limitation in scope, material change, or non-renewal of any insurance coverage right away (but no later than five (5) business days of receiving notice from the insurer).

(2) University insurance not primary. Insurance obtained by Contractor and/or any Contractor Agents pursuant to this contract will be primary and any University insurance will apply only in excess of and not

contribute with such insurance obtained by Contractor and/or any Contractor Agents.

- (3) Name University as an additional insured. University shall be named as an additional insured on all insurance coverage that Contractor and/or any Contractor Agent is required to obtain under the Contract except for workers compensation and employers liability insurance.
  - (4) Waiver of subrogation. All insurance obtained by Contractor will contain a waiver of subrogation endorsement in favor of University.
  - (5) University not required to pay premiums. Contractor and Contractor Agents will be responsible for paying all costs associated with obtaining the required insurance coverage described in the contract, including all premiums. University will not be responsible for paying any such costs.
  - (6) Acceptable deductibles. The terms and amounts of any deductibles for the required insurance coverage under the contract must be reasonable and acceptable to University based upon the type of insurance involved and the conduct of the services.
- C. Deposit insurance certificates. Contractor will timely deposit and keep on deposit with University, certificates of insurance necessary to satisfy University that the insurance requirements of the contract have been and continue to be satisfied during the term of the contract.
- D. University may cure failure to obtain/maintain insurance. If Contractor fails to provide and maintain the insurance required by the contract after written notice to comply from University, University may, but shall not be required to, procure such insurance at the sole cost and expense of Contractor, who shall be obligated to immediately reimburse University for the cost thereof plus ten percent (10%) to cover University's administrative overhead.
- E. Lapse in insurance constitutes a breach. Any lapse in, or failure by Contractor or any Contractor Agents to procure and maintain the insurance coverage required under the contract, at any time during and throughout the term of the contract, shall be a breach of the contract and University may terminate the rights of Contractor and all Contractor Agents to conduct the services.
- F. Insurance shall not limit Contractor liability. Obtaining the required insurance coverage will not be construed to limit Contractor's liability hereunder or to fulfill Contractor's indemnification, defense, and hold harmless obligations under the contract. Notwithstanding the required insurance coverage, Contractor shall be obligated for the full and total amount of any damage, injury, or loss arising from acts or omissions of Contractor and/or the Contractor Agents.

- G. University may adjust insurance requirements. University may, upon reasonable notice and reasonable grounds, increase or change the form, type, coverage, or coverage limits of the insurance required hereunder, in which event Contractor shall, and shall cause the Contractor Agents to, obtain insurance, as modified. University's requirements shall be reasonable and shall be designed to provide protection against the kind and extent of risks that exist at the time a change in insurance is required. Contractor shall satisfy all University risk management requirements that are in effect as of the Effective Date and as may be amended from time to time.

#### 5.12 ESCALATION CLAUSE

During the initial FIVE (5) year term of the CONTRACT, the CONTRACT prices for the licensing fees and implementation services shall be in accordance with the pricing provided in the CONTRACTOR'S PROPOSAL. After the initial FIVE (5) year term, the CONTRACTOR shall be allowed to request adjustments to the CONTRACT price for licensing fees, NINETY (90) days prior to the CONTRACT renewal date, provided that the CONTRACT price for each renewal period shall not increase more than FIVE (5)% (or) more than the Consumer Price Index for Pacific Cities and U. S. City Average based on All Urban Consumers, U. S. City Average, in effect ONE HUNDRED TWENTY (120) days prior to the renewal date, whichever is less, and provided further, that the request is made in writing to the UNIVERSITY.

#### 5.13 PAYMENT

- A. The termination of the CONTRACT by default or otherwise shall not relieve the CONTRACTOR or UNIVERSITY of their obligations under the contract or for charges accrued while the CONTRACT was in effect but remaining unpaid at the time of termination.
- B. Any amounts owing by the CONTRACTOR under the terms of the CONTRACT shall bear interest from the date such amounts become due until paid. The rate of such interest shall be either (a) at the specific maximum rate, if any, then allowed by the appropriate sections of statutes of Hawaii, or any successor law or statute, or (b) if there is no such maximum rate, TWO (2) percentage points above the large business prime rate of interest then being charged by the bank principally used by the UNIVERSITY.
- C. The Contractor shall be remunerated upon submission of a properly executed original invoice and ONE (1) copy, indicating the contract number, to Information Technology Services, University of Hawaii, 2520 Correa Road, IT Center, 5<sup>th</sup> Floor, Honolulu, Hawaii 96822.

#### 5.14 SOFTWARE LICENSE AGREEMENTS

The University will execute Software License Agreements, if necessary, as long as the terms and conditions of the License Agreements do not conflict with the terms and conditions of this Request for Proposals. Inasmuch as the Contractor will be selecting the software for the University, the standard waivers of warranties of merchantability and fitness for a particular purpose shall not be accepted. The University shall be protected from claims of copyright infringement not occasioned by University modification of the software. The University will not execute software license agreements with third parties.

## ATTACHMENT A

### Headcount Enrollment (CENSUS) AY 2023-2024

<u>Campus</u>	<u>Headcount Fall 2022</u>	<u>Headcount Spring 2023</u>
UH Mānoa	19,256	18,324
UH Hilo	2,781	2,587
UH West O'ahu	2,863	2,763
Hawai'i Community College	2,260	2,154
Honolulu Community College	3,204	2,951
Kapi'olani Community College	5,822	5,439
Kaua'i Community College	1,298	1,214
Leeward Community College	6,059	5,973
UH Maui College	2,647	2,435
Windward Community College	2,743	2,578
<b>Total</b>	<b>48,933</b>	<b>46,418</b>

Source: University of Hawai'i Institutional Research, Analysis and Planning Office (IRAPO), [Headcount Enrollment Multi-Year University of Hawai'i](#)

## **ATTACHMENT B**

### Faculty Count by Campus Fall 2023

<u>Campus</u>	<u>Full-time Instructional Faculty</u>	<u>Part-time Lecturers</u>	<u>Total</u>
UH Mānoa	1,302	348	1,650
UH Hilo	178	75	253
UH West O'ahu	88	88	176
Subtotal (Universities)	1,568	511	2,079
Hawai'i Community College	63	77	140
Honolulu Community College	72	56	128
Kapi'olani Community College	166	110	278
Kaua'i Community College	44	33	77
Leeward Community College	117	99	216
UH Maui College	61	87	148
Windward Community College	46	55	101
Subtotal (Community Colleges)	569	517	1,086
<b>Total</b>	<b>2,137</b>	<b>1,028</b>	<b>3,165</b>

Source: IRAPO, [Faculty and Staff Report, Number of Personnel and FTE, Fall 2023](#)

## ATTACHMENT C

### University of Hawai'i Employee FTE Sept 2023- August 2024

<u>Time interval</u>	<u>Regular FTE</u>	<u>Casual FTE</u>	<u>Total FTE</u>
09/23 - 12/23	7,736	440	8,176
01/24 - 03/24	7,861	514	8,375
04/24 - 06/24	7,411	444	7,855
07/24 - 08/24	7,542	533	8,075
<b>1yr Average of FTE</b>			<b>8,121</b>

Source: Office of Human Resources from UH's PeopleSoft HR S

## PROPOSAL APPENDIX FORMS

This document indicates the proposal requirements for the RFP which shall be submitted by the deadline set for submission of proposals. Offeror shall complete the appropriate proposal requirements, sign all appropriate forms, and attach (upload) the completed Appendixes to their HlePRO online RFP submission.

### **APPENDIX CHECKLIST**

THE FOLLOWING APPENDIXES IN THIS TABLE MUST BE COMPLETED AS PART OF THE RFP AND SHALL BE UPLOADED WITH THE OFFERORS HlePRO SUBMISSION.

<b>APPENDIX DESCRIPTION</b>	<b>APPENDIX</b>
Proposal Letter	Appendix A
Business Classification Certification Statement	Appendix B
Price Quotation Sheet	Appendix C
Executive Summary	Appendix D
Company History and Organization	Appendix E
Product Roadmap	Appendix F
Offeror Minimum Qualification Matrix	Appendix G
Technical and Data Capabilities	Appendix H
Key Features	Appendix I
Training and Support	Appendix J
Data Sharing Protections and Requirement Capabilities	Appendix K
Implementation Plan	Appendix L
References	Appendix M

The University is not responsible for any issues with the uploading of the Appendixes into HlePRO.



**APPENDIX A  
PROPOSAL LETTER  
UNIVERSITY OF HAWAII**

We propose to provide the Digital Badging/Micro-Credential solution named in the Request for Proposals (RFP) No. 25-2294 to Provide a Digital Badging/Miro-Credential Solution for University of Hawaii System, Honolulu, Hawaii.

It is understood that this proposal constitutes an offer.

It is understood and agreed that we have read the University of Hawaii's specifications described in the RFP and that this proposal is made in accordance with the provisions of such specifications. By signing this proposal, we guarantee and certify that all items included in this proposal meet or exceed any and all such specifications.

We agree, if awarded the contract, to deliver goods or services which meet or exceed the specifications.

Respectfully submitted,

\_\_\_\_\_  
Legal Name of Offeror

\_\_\_\_\_  
Date

\_\_\_\_\_  
Authorized Signature (original)      **(Typed Name)**

\_\_\_\_\_  
Title

\_\_\_\_\_  
Street Address

\_\_\_\_\_  
Telephone No.

\_\_\_\_\_  
City, State, Zip Code

\_\_\_\_\_  
Fax No.

\_\_\_\_\_  
Social Security OR Federal Tax Payer ID No.

\_\_\_\_\_  
Email

\_\_\_\_\_  
Remittance Address (if different from street address)

\_\_\_\_\_  
Hawaii General Excise Tax License No.

\_\_\_\_\_  
City, State, Zip Code

\_\_\_\_\_  
Location of Offeror's Plant

Offeror is:       Individual     Partnership     Corporation\*     Joint Venture

State of Incorporation:     Hawaii     Other:

Is Corporate Seal Available In Hawaii:     Yes\*\*     No

\*      Attach to this page evidence of authority of the above officer to submit an offer on behalf of the corporation, giving also, the names and addresses of the other officers.

\*\*      If yes, affix corporate seal

### APPENDIX B BUSINESS CLASSIFICATION CERTIFICATION STATEMENT

**CONTRACTORS: Please complete the information below.** Terms used are taken from the U.S. Small Business Administration (SBA) Rules and Regulations (<https://www.sba.gov/>) and the U.S. Code of Federal Regulations (CFR). The term “controlled” refers to the management and daily operation of the business concern.

The company identified below (check all that apply):

- 1. \_\_\_\_\_ **IS NOT** a small business concern as defined in the regulations  
**(If you checked here, STOP. GO TO CERTIFICATION BELOW.)**
- \_\_\_\_\_ **IS a small business concern**, defined as one that is independently owned and operated, is organized for profit, is not dominant in its field, meets the SBA size standard eligibility (see reverse side of this form for examples of size standards), is registered and has its status represented in the U.S. Government’s System for Award Management (SAM) database. See <http://www.sba.gov/content/what-sbas-definition-small-business-concern>.
- 2. \_\_\_\_\_ IS a **small disadvantaged business concern** of which at least 51% is unconditionally and directly owned and controlled by one or more socially disadvantaged and economically disadvantaged persons who are U.S. citizens. See 13 CFR 124.105 for exceptions.
- 3. \_\_\_\_\_ IS a **women-owned small business concern** of which at least 51% is unconditionally and directly owned and controlled by one or more women who are U.S. citizens. See 13 CFR 127.
- 4. \_\_\_\_\_ IS a **HUBZone small business concern** that meets the certification eligibility requirements set by the U.S. SBA. See 13 CFR 126.
- 5. \_\_\_\_\_ IS a **veteran-owned small business concern** of which at least at least 51% is unconditionally and directly owned by one or more veterans or service-disabled veterans. See 38 CFR 74.
- 6. \_\_\_\_\_ IS a **service-disabled veteran-owned small business concern** of which at least 51% is unconditionally and directly owned by one or more service-disabled veterans. In the case of any publicly owned business, not less than 51% of the stock of which is owned by one or more service-disabled veterans. The management and daily business operations of which are controlled by one or more service-disabled veterans, or in the case of a veteran with a permanent and severe disability, a spouse or permanent caregiver of such veteran. See 13 CFR 125.11 et al.

#### CERTIFICATION

I hereby certify the information supplied herein to be true and correct. (Any misrepresentation shall be subject to the provisions stated in item B on the next page.)

Company Name: \_\_\_\_\_

\_\_\_\_\_  
Signature of Company Officer

Company Address: \_\_\_\_\_

Print Name: \_\_\_\_\_

\_\_\_\_\_

Title: \_\_\_\_\_

\_\_\_\_\_

Date: \_\_\_\_\_

Type of Goods/Services: \_\_\_\_\_

North American Industry Classification System (NAICS) Code: \_\_\_\_\_

## APPENDIX B

A. A small business concern is one that is independently owned and operated, is organized for profit, is not dominant in its field, has a place of business in the U.S., and operates primarily within the U.S. or makes a significant contribution to the U.S. economy. Size standard eligibility is based on the average number of employees for the preceding 12 months or on sales volume averaged over a 3-year period. See 13 CFR 121.201 for size standards identified by NAICS codes. The size standards for a few industries are shown below and are subject to change at any time.

1. SPECIALTY TRADE CONTRACTORS – “Small” if average annual receipts for preceding 3 years do not exceed \$15 million.
2. CONSTRUCTION, GENERAL CONTRACTORS – “Small” if average annual receipts for preceding 3 years do not exceed \$36.5 million.
3. MANUFACTURING – “Small” if 500 employees or less, except for some specific products which will increase the complement of employees to 750 or 1,000.
4. TRANSPORTATION – “Small” if average annual receipts for preceding 3 years do not exceed the amount shown for specific services.

\$27.5 million – general freight trucking, local.

5. WHOLESALE TRADE, DURABLE AND NON-DURABLE GOODS – “Small” if 100 employees or less.
6. RETAIL TRADE – “Small” if average annual receipts for preceding 3 years do not exceed the amount shown for specific products.

\$7.5 million – hardware stores.

7. SERVICES – “Small” if average annual receipts for preceding 3 years do not exceed the amount shown for specific services:
  - a) \$27.5 million – computer systems design services, custom computer programming services  
\$20.5 million – security guards and patrol services
  - b) \$18 million – janitorial services
  - c) \$38.5 million – passenger car rental
  - d) \$32.5 million – office machinery and equipment rental & leasing
  - e) \$7.5 million – general automotive repair

Annual receipts of a concern which has been in business for less than 3 complete fiscal years means the total receipts for the period the concern has been in business divided by the number of weeks in business, multiplied by 52. See 13 CFR 121.104.

B. Notice. Under 15 U.S.C. 645(d), any person who misrepresents a firm’s status as a small business concern, a qualified HUBZone small business concern, a small business concern owned and controlled by socially and economically disadvantaged individuals, or a small business concern owned and controlled by women in order to obtain a contract to be awarded under the preference programs established pursuant to 15 U.S.C. sections 637(a), 637(d), 638, 644, or 657(a), shall:

1. Be punished by imposition of fine, imprisonment, or both;
2. Be subject to administrative remedies including suspension and debarment; and
3. Be ineligible for participation in a program conducted under the authority of the Small Business Investment Act of 1958.

**APPENDIX C  
UNIVERSITY OF HAWAII  
PRICE QUOTATION SHEET**

Complete the worksheet as follows.

1. Provide a price quote for the digital badging/micro-credentials solution based on the information provided in Appendices D through K, which shall include the following:
  - A. Licensing fees based on the user-type and number of users. Refer to ATTACHMENTS A, B and C to determine the number of licenses based on Headcount Enrollment, Faculty Count, Employee FTE. Licensing fees shall commence upon satisfactory implementation and acceptance of the digital badging/micro-credentials platform and shall be projected out for a FIVE (5) year term in accordance with the estimated implementation timeline in Section 2.9 and thereafter paid on a fixed, annual basis.
  - B. One (1) – time fees for implementation services (e.g., Configuration and Testing integrations, Partnership, Training and Support) that the Offeror is providing to the University. One (1) – time fees shall be assessed to the University in accordance with the estimated implementation timeline in Section 2.9.
  - C. All fees shall include hardware, software, maintenance, mobile application costs, man-hours, travel-related expenses, overhead, and all applicable fees and taxes.

2. All rows in the worksheet must be completed. If there are no costs associated for any item, a “N/A” designation shall be indicated and the Offeror is not to assess any cost for that line item.

Cost for License Fees. <b><u>ANNUAL FEES</u></b>							
No.	Description	Year 1: Headcount Enrollment, Faculty Count, Employee FTE.	Year 2: Headcount Enrollment, Faculty Count, Employee FTE.	Year 3: Headcount Enrollment, Faculty Count, Employee FTE.	Year 4: Headcount Enrollment, Faculty Count, Employee FTE.	Year 5: Headcount Enrollment, Faculty Count, Employee FTE.	Total
1.	License Fee						
	<b>Total Annual Fees</b>						
<b><u>ONE-TIME FEES</u></b>							
No.	Description	One-Time Fee					
1.	Implementation Services: A. System Configuration and Testing Integrations B. Partnership C. Training D. Support						
	<b>Total One-Time Fees</b>						
<b>TOTAL PRICE:</b>							

**APPENDIX D  
EXECUTIVE SUMMARY**

Provide an Executive Summary that includes a brief overview of Offeror's proposal summarizing the anticipated results, as well as an overview of the process that the Offeror intends to follow to achieve these results.

**APPENDIX E  
COMPANY HISTORY AND ORGANIZATION**

Provide information regarding Offeror's company history and organization in the following areas:

1. Provide company headquarters information.
2. Provide company ownership structure.
3. Provide the number of years in business.
4. Provide awards and merits.
5. Provide software evolution and direction.
6. Provide evidence of financial stability.
7. Provide previous experience implementing projects similar in scope.

## **APPENDIX F PRODUCT ROADMAP**

Provide Offeror's plan for future updates to the solution as they relate to the following questions:

1. Describe how items are prioritized on the product roadmap.
2. How often is the product roadmap updated.
3. How often is the product roadmap made publicly available and/or available to partnering institutions.



**APPENDIX G  
OFFEROR MINIMUM QUALIFICATION MATRIX**

<b>Offeror Company Name:</b>	
<b>1. Cybersecurity and Disaster Recovery Plans</b>	<b>Yes/No</b>
<b>Indicate “Yes” or “No” if the Offeror possesses the following qualifications, and furnish the corresponding documents:</b>	
SOC 2 certification (the University’s CISO can sign a Non-Disclosure Agreement)	
Privacy policy or statement, including FERPA compliance	
Security plans and practices	
DATA flow diagram	
Network architecture diagram	
Disaster recovery plan	
<b>2. Standards-Based Compliance</b>	
<b>Indicate “Yes” or “No” if the following certifications of the Offeror are verifiable through 1EdTech (available at 1edtech.org). If “No”, furnish an alternative certification with a detailed explanation of how the alternative certification is comparable to the certification through 1EdTech.</b>	
Open Badges v. 2.0 or v.3.0 Type: issuer, Displayer, Host	
Open Badges v: 2.1 or v.3.0 API Support Service Provider	

<b>3. Demonstrate Ability</b>  Indicate “Yes” or “No” if the Offeror possesses the following qualifications, and furnish the corresponding documents:	
Accessibility Conformance Report completed utilizing Voluntary Product Accessibility Template VPAT 2.3 and Web Content Accessibility Guidelines (WCAG 2.1). The accessibility evaluation submitted must correspond to the current version of the proposed SOLUTION.	
Comprehensive accessibility evaluation from an objective, independent third party verifying the claims made on the product Accessibility Conformance Report (VPAT 2.3), or equivalent, if an independent third party did not complete the Accessibility Conformance Report. OFFEROR may use a third-party accessibility evaluation service of their choice.	
<b>3. Accessibility</b>  Indicate “Yes” or “No” if the Offeror has the following documents, and furnish the corresponding documents:	
Accessibility Conformance Report	
Accessibility Evaluation	

## **APPENDIX H TECHNICAL AND DATA CAPABILITIES**

Provide details on how the Offeror's solution meets the technical and data requirements of the University as referred to in Section 2.5, and also address specific issues as follows:

1. Describe how the solution functions across various web browsers.
2. Describe how the solution runs natively and responsively across various device types (e.g., desktop, laptop, tablet, smartphone).
3. Describe the availability of a mobile application for the solution.
4. Describe any limitations or differences in functionality for digital badge display and sharing between the website and the mobile application.
5. Describe in detail the integration capabilities between the solution and Brightspace learning management system.
6. Describe how the solution integrates with the University's Non-Credit Student Information System, Modern Campus.
7. Describe how the solution integrates with the University's Student Information System, Ellucian-Banner.
8. Describe how the solution supports the University's SSO.
9. Describe how the solution supports Two-Factor MFA.
10. Indicate where the application is hosted and where the data is hosted.
11. Describe where the data is hosted.
12. Describe the server response time, uptime guarantees, and maintenance schedule.
13. Describe the storage capacity and storage management support.
14. Describe how the solution will handle virus-infected (e.g., malware) files.
15. Describe how virus-infected files will be identified and quarantined or remediated when uploaded to the solution.
16. List and describe any security breaches and incidents compromising confidential information during the last FIVE (5) years.

17. Indicate any content or solution areas that are restricted system administrator access.
18. Describe in detail the types of reporting and analytic capabilities of the solution.
19. Describe in detail the solution's web accessible content features.

## **APPENDIX I KEY FEATURES**

Provide details on how the Offeror's solution meets the key feature requirements of the University as referred to in Section 2.6, summarized as follows:

1. Badge Hosting and Issuing
2. Open Badges Standards
3. Digital Badge Issuer User Interface
4. Metadata
5. Digital Badge Earner Capabilities
6. FERPA Compliance

**APPENDIX J  
TRAINING AND SUPPORT**

Offeror shall provide details on training and support provided for the solution as referred to in Section 2.7.

1. Describe the training and support provided for badge issuers.
2. Describe the training and support provided for badge earners.
3. Describe ongoing technical support for badge issuers and badge earners.

**APPENDIX K**  
**DATA SHARING PROTECTIONS AND REQUIREMENTS CAPABILITIES**

Provide a data sharing protections plan that provides details on how the Offeror's solution meets the data sharing protections and requirements of the University as referred to in Section 2.8, and shall also address specific issues as follows:

1. Describe the transmission of data and network security based on the data flow diagram and network architecture diagram referenced in Section 2.9 and Appendix G.
2. Describe the Offeror's data confidentiality policies.
3. Describe the Offeror's application security such as software update, upgrades, and patch schedules.
4. Describe how the Offeror will fulfill the elements described in Section 2.8, Sub-item G, Data Security.
5. Describe the Offeror's policies and/or procedures around disclosures to third parties.
6. Describe the Offeror's policies and/or procedures around destruction of data.
7. Describe the Offeror's policies and/or procedures around data breaches and mandatory disclosures of PII, as evidenced by incident response and data breach procedures.

## **APPENDIX L IMPLEMENTATION PLAN**

Provide a detailed implementation plan based on the estimated implementation timeline in Section 2.9, which shall also address specific issues as follows:

1. Describe the technical assistance provided with managing system configuration, branding, and establishing integrations with the hosting service provider.
2. Describe the technical assistance provided with the solution's system configuration and organizational hierarchy.
3. Describe the support provided for testing the integration with the University's Student Information System, multi-factor authentication system.
4. Describe the technical assistance, documentation, and resources to support stake holder engagement.
5. Describe the resources provided for an ongoing partnership with the University throughout the term of the contract to respond to feedback and address technical and functional questions and concerns related to the solution, support, and product enhancements.
6. Describe the resources provided for ongoing technical support to digital badge issuers and Information Technology Services Help Desk managers.



7. Complete the following table, outlining the tasks involved with the implementation of the solution as referenced to in Section 2.9, including the start and end dates of each task, description of the resources required and/or provided, and the responsible party for each task.

Task	Task Description	Start Date	End Date	Resource

**APPENDIX M  
REFERENCES**

Provide the information for THREE (3) references. Refer to Section 3.14 for further information.

**Reference 1**

Name of Institution: \_\_\_\_\_

Address: \_\_\_\_\_  
\_\_\_\_\_

Contact Name: \_\_\_\_\_ Position: \_\_\_\_\_

Telephone Number: \_\_\_\_\_ Email address: \_\_\_\_\_

FTE: \_\_\_\_\_ Cost: \_\_\_\_\_

Description of Services Provided:

**Reference 2**

Name of Institution: \_\_\_\_\_

Address: \_\_\_\_\_  
\_\_\_\_\_

Contact Name: \_\_\_\_\_ Position: \_\_\_\_\_

Telephone Number: \_\_\_\_\_ Email address: \_\_\_\_\_

FTE: \_\_\_\_\_ Cost: \_\_\_\_\_

Description of Services Provided:

**Reference 3**

Name of Institution: \_\_\_\_\_

Address: \_\_\_\_\_

\_\_\_\_\_

Contact Name: \_\_\_\_\_ Position: \_\_\_\_\_

Telephone Number: \_\_\_\_\_ Email address: \_\_\_\_\_

FTE: \_\_\_\_\_ Cost: \_\_\_\_\_

Description of Services Provided: