STATE OF NORTH CAROLINA Central Piedmont Community College	**REQUEST FOR INFORMATION NO**. 88-260022-JE Due Date: May 18, 2026 by 2pm
Refer ALL Inquiries to: Jennifer Ennis	Issue Date: April 23, 2026 Commodity: 811620 – Software as a Service
E-Mail: jennifer.ennis@cpcc.edu	Using Agency Name: Central Piedmont Community College

SUBMITTAL INSTRUCTIONS: Responses to this Request for Information (RFI) shall be submitted via the electronic vendor portal (eVP) by the due date and time specified herein. Additional information can be found at https://evp.nc.gov/.

NOTICE TO VENDOR

Request for Information (RFI) responses will be received electronically via the electronic Vendor Portal (eVP) until May 18, 2026 at 2pm on the day of opening and then opened. Additional information can be found at the eVP updates for Vendors link: https://eprocurement.nc.gov/news-events/evp-updates-vendors

EXECUTION

VENDOR NAME:	E-MAIL:	
STREET ADDRESS:	P.O. BOX:	ZIP:
CITY & STATE:	TELEPHONE NUMBER:	TOLL FREE TEL. NO:
TYPE OR PRINT NAME & TITLE OF PERSON SIGNING:	FAX NUMBER:	
AUTHORIZED SIGNATURE:	DATE:	

1.0 EXECUTIVE SUMMARY

1.1 Introduction:

Central Piedmont Community College (Central Piedmont) is a large, urban, multi-campus, non-residential college that enrolls more than 52,000 students annually in curriculum, adult high school and basic skills, and continuing education programs, and employs more than 3,000 full- and part-time faculty and staff, making Central Piedmont one of the largest colleges in the Carolinas. Central Piedmont offers more than 300-degree, diploma and certification programs, customized and corporate training, market-focused continuing education, and special interest classes. Central Piedmont is academically, financially, and geographically accessible to all citizens of Mecklenburg County. Central Piedmont responds to the workforce and technology needs of local employers and job seekers through innovative educational and training strategies. Established in 1963, Central Piedmont has provided over 60 years of service to Mecklenburg County residents, business and industry engaging approximately 250,000 people each year through various programs, services, events, and performances.

1.2 Purpose:

The Public Safety training program currently relies on outdated, paper-based processes for class registration, attendance tracking, instructor timesheets, and payroll. These manual processes are time-consuming, prone to errors and require significant administrative effort – often exceeding 20 hours per week for payroll alone. With the opening of the new Public Safety Training Facility in 2027, the program must advance significantly to align with modern training standards. A user-friendly, automated system is essential to streamline workflows, improve data accuracy, reduce administrative workload, and support high-volume training across multiple locations, ensuring the program can fully leverage the capabilities of the new facility.

Central Piedmont Community College is conducting industry research to learn more about available platforms in that market that automate and streamline the workflows noted above.

2.0 RFI PROCEDURES

2.1 Schedule

Respondents will have three weeks to prepare their submissions to this RFI. Responses must be received by the date, time and the location specified on the cover sheet of this RFI. There is no guarantee that all RFI submissions will be invited to present. If selected, respondents will be notified of the specific date and time approximately two weeks in advance of their presentation.

Intended Schedule of Events

All times listed are EST.

April 23, 2026	RFI issued
May 1, 2026, 2pm	Written questions due
May 6, 2026	Response to Written Questions (via electronic vendor portal)

May 18, 2026, 2pm Submission of Information due

2.2 RFI Related Questions/Clarifications

Any questions regarding this RFI should be emailed on or before May 1, 2026 at 2:00 pm EST to the attention of: jennifer.ennis@cpcc.edu. All questions must be submitted in writing. Please enter "Questions RFI 88-260022-JE" as the subject for the email. An addendum containing any general clarification questions and their answers will be issued as an addendum to this RFI within the electronic vendor portal (eVP).

Vendors responding to the RFI shall designate a single contact within that company for receipt of all subsequent information regarding this RFI.

3.0 RFI SPECIFICATIONS

The College expects concise, detailed, point-by-point responses to each of the RFI response items identified in Section 4.0 of this RFI. The College is not interested in brochures or "boilerplate" responses. Instead, responses should clearly define how the vendor's proposed solution(s) would meet the College's business requirements. Any issues or exceptions to the College's requirements should also be identified and explained.

3.1 Format of RFI Responses

The following outline is offered to assist in the development of your response.

- A cover letter -- the cover letter should include a brief summary of your response, such as indicating to which areas you are responding and must also indicate if supporting documentation is included in your response.
- The response itself, covering any or all of the areas of information requested by this RFI should be saved in a .pdf format.
- Although the College does not limit the size of responses, you are asked to consider that the College will rely upon staff with limited time availability to review these responses. In order to assure that your response receives the attention it deserves, you are asked to consider limiting the size of your response (not counting any supporting documentation) to approximately 20 pages. If you consider supporting documentation to be necessary, please indicate which portions of the supporting documentation are relevant to this RFI.
- The State recognizes that considerable effort will be required in preparing a response to this RFI. **However, please note this is a request for information only, and not a request for services**. The Vendor shall bear all costs for preparing this RFI.
- Multiple responses will be accepted from a single vendor provided that each response is comprehensive, meets all the state's requirements, and is truly unique. Please clearly mark responses as "Response #1, Response #2, etc.

A comprehensive, detailed equipment list including software required for the proposed solution should be provided. While the State may require a pilot installation of any final solution adopted, the State is not interested in participating in any field trials of new software.

The response should define all services that would be required by the proposed solution. The response should also include:

- The vendor's understanding of the project and services by addressing the State's business requirements;
- An estimated total cost of ownership for the solution including continued compliance with emerging industry standards.

Responses to the Request for Information (RFI) will help the college to:

- Decide whether to issue a solicitation,
- Determine the scope of work, and implementation timelines

4.0 AUTOMATED WORKFLOW SOLUTION SCOPE

4.1 Business Requirements

Needing an easy-to-use scheduling and registration platform that includes:

- Single Sign-On (SSO) using Microsoft Entra ID
- Integration with Colleague/Self-Service
- Potential integration with Canvas, and Element 451 using standard REST API architecture
- User-friendly, intuitive, and efficient interface
- Mobile-friendly design

Key features should include:

- Streamlined Process: A streamlined and efficient process that streamlines class scheduling, registration, attendance and payroll reporting, resource allocation, and integrates with records management systems. .
- Campus and Modality Filters:
  - Ability to designate specific campus locations and filter schedules by multiple start dates

  Filter by multiple modalities such as:
  - In-person classes
  - Online classes
  - Hybrid classes
  - Synchronous classes
  - Asynchronous classes
  - Auditing, reporting, workflows

This Request for Information (RFI) is intended to collect information and recommendations, including but not limited to, software solutions that provide:

- Minimize manual work hours: Reduce the significant time spent on paper-based processes, data entry, and administrative tasks by implementing digital class creation, automated registration, QR code check-ins, and streamlined instructor/facilitator tracking, freeing staff to focus on higher-value activities.
- Ease of use: Implement a user-friendly, app-based system that simplifies workflows for learners, instructors, and administrators, making it intuitive to navigate while reducing the need for extensive training, and providing automated notifications for schedule or location changes to keep everyone informed effortlessly.
- Minimize human error: Automate repetitive tasks and data entry through digital registration, integrated records management, and automated attendance and payroll tracking to reduce errors and improve overall accuracy. Automation of forms, attendance, and payroll: Replace manual processes with digital registration, timesheets, QR code attendance, and payroll submission, incorporating robust audit capabilities to streamline operations, improve data accuracy, and ensure real-time reporting and compliance. Enable enrollees to access course materials using their personal credentials rather than requiring a Central Piedmont ID. This change will simplify the login process, reduce barriers to access, and improve the overall user experience for enrollees and their employers. By minimizing the need to manage multiple logins, the solution is expected to increase enrollment satisfaction, decrease support requests for login issues, and streamline administrative processes.

4.2 Security Expectations

a) Data Encryption
   i) How does your solution protect sensitive data at rest and in transit, and what encryption standards are used?
b) Cyber Resilience:
   i) How does your solution securely integrate with third-party applications or services, including authentication, authorization, and data protection controls?
   ii) What independent security assessments (e.g., penetration testing, third-party reviews) are conducted, and how frequently?
c) Incident Response
   i) Describe your incident response program, including how security incidents are detected, managed, and resolved.
   ii) Provide a summary of any material security incidents or data breaches in the past five years and the corrective actions taken. Promptly notify us of any security issues, updates, or reports concerning the solution and our data within it, ensuring transparent communication.
d) Compliance Requirements
   i) How does your solution support FERPA requirements for protecting student data, and can you provide a current SOC 2 Type II report?
   ii) Establish clear data retention and secure deletion/anonymization policies for unnecessary sensitive data, with written proof of data deletion within 24 hours.
e) Access Control
   i) Implement robust authentication mechanisms, including single sign-on (SSO) and multi-factor authentication (MFA), alongside role-based access control (RBAC), to restrict access based on roles.
   ii) Adhere to the principle of least privilege and segregation of duties.
f) Continuous Monitoring
   i) What logging and monitoring capabilities are provided, including visibility into user and administrative activity? How does your solution support integration with enterprise monitoring or SIEM platforms such as Splunk Enterprise Security?
g) Third-Party Security
   i) What third-party services or subprocessors are used, and what role do they play in delivering the solution?

4.3 Software Standards

a) *Endpoint installed*

i. Supports Windows 11, or macOS/iPadOS within one major version of the latest vendor release.
ii. Compatible with ITS application management platforms: Jamf, Intune
iii. Solution must support deployment via Citrix or Azure VDI (if virtualization is required)
iv. Does not require the end-user to have local administrator role

b) College hosted

i. Compatible with Microsoft Azure virtualization standards (e.g., Hyper-V, Azure-hosted VMs)
ii. Supports current standard MS Windows Server or Redhat Enterprise Linux version
iii. Must support Azure SQL Managed Instance (if database required)

c) SaaS

i. Vendor-guided implementation and ITS project request required
ii. Must support enterprise licensing model (no single-payer credit card subscriptions)

d) Compatibility and standards

i. Meets or exceeds accessibility standard WCAG2.1 AA
ii. Supports latest version of Microsoft Edge and other Chromium-based browsers
iii. Supports delivery of software updates via ITS application management platforms (e.g., Intune).

e) *Identity and Access*

i. Supports SAML2 and/or Microsoft Entra ID SSO
ii. Includes role-based access permissions
iii. Supports group-based role provisioning via SCIM, Entra ID, or API integration
iv. Administrator access requires SSO if supported; local admin logins require MFA

f) Data and integration

i. Integration methods: Ellucian Ethos, WebAPI, or structured data file transfer
ii. College data must be stored in USA
iii. Vendor must comply with all applicable regulations (e.g. FERPA)
iv. Solution supports data export in non-proprietary forms (e.g. JSON, CSV)

Other Standards

a) Networking

i. Wi-Fi connectivity must support 802.1x or WPA2-PSK for Wi-Fi authentication and be compatible with 802.11ac / Wi-Fi 5
ii. Wired connectivity must support 100/1000Mbps RJ45 Ethernet
iii. Power Over Ethernet requirements must not exceed 30W (PoE+)
iv. Must support enterprise networking capabilities (e.g., routable across VLANs, compatible with DHCP and DNS)
v. Must support encrypted protocols such as HTTPS, SMBv3, and SSH

a) Support

i. Vendor provided technical support with defined escalation paths and SLA
ii. Vendor provided end-user and technical documentation
iii. Vendor provided implementation and configuration assistance
iv. Solution must support automated delivery of firmware and software updates via enterprise app management platforms (e.g., Intune, Jamf, SCCM) or native OTA (over-the-air) update mechanisms.