RANCHO SANTIAGO COMMUNITY COLLEGE DISTRICT
Website: Technology Advisory Group

Agenda for October 3, 2024
2:30 p.m. - 4:00 p.m.
https://rsccd-edu.zoom.us/j/89891073164

1. TAG Accomplishments and Goals:
   - Review of 2023-2024 TAG Accomplishments (5 minutes) – Gonzalez
   - Approval of TAG goals for 2024-2025 (5 minutes) – **ACTION**– Gonzalez

2. First reading, updates to AR 3720, Computer and Network Use (5 minutes) – Gonzalez

3. Approval of Strategic Technology Plan Task Force membership (5 minutes) – **ACTION**– Gonzalez

4. Approval of computing standards (10 minutes) **– ACTION**– Gonzalves

5. Proposals to add to contract renewal costs for next Fiscal Year (10 minutes) – Gonzalez

6. Technology Update – Colleges
   - SACTAC – Steffens (10 minutes)
   - SCCTEC – Rodriguez (10 minutes)

7. Student experience with technology:
   - SAC – Mondragon-Rosas – (10 minutes)
   - SCC – Lopez – (10 minutes)

8. Approval of TAG Minutes – September 5, 2024 (5 minutes) **– ACTION**– Gonzalez

9. Technology Project listing, September 2024 (5 minutes) – Howard

Next TAG Committee Meeting: November 7, 2024

The Rancho Santiago Community College District aspires to provide equitable, exemplary educational programs and services in safe, inclusive, and supportive learning environments that empower our diverse students and communities to achieve their personal, professional, and academic goals.

TAG Accomplishments 2023-2024

1. Approved and adopted Districtwide Initiatives for FY 2024-2025 into the Strategic Technology Plan.
2. Maintained computing standards updated.
3. Aligned planning cycles for all Strategic Technology Plans.
4. Verified that progress occurs on student produced initiatives, computer replacement plan, accessibility and data privacy initiatives.
5. Updated AR 3750.1, Data Governance.
6. Provided recommendation on the districtwide use of Zoom AI.

TAG Goals 2024-2025

1. Develop 2025-2029 Strategic Technology Plan.
2. Maintain updated computing standards.
3. Verify that progress occurs on student produced initiatives, computer replacement plan, accessibility and data privacy initiatives.
4. Update or produce Administrative Regulations guiding the use of technology.

Rancho Santiago Community College District
ADMINISTRATIVE REGULATION
Chapter 3
General Institution

AR 3720 Information Resources Acceptable Use

References

15 U.S. Code Sections 6801 et seq.
17 U.S. Code Sections 101 et seq.
Penal Code Section 502, Cal. Const., Art. 1 Section 1
Government Code Section 3542.1 subdivision (b)
16 Code of Federal Regulations Parts 314.1 et seq.
Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45

1.0 Purpose and Scope

The objective of this administrative regulation is to outline the acceptable use of information resources at Rancho Santiago Community College District ("District"). Inappropriate use exposes the District to risks including compromise of network systems and services or legal issues.

This regulation applies to all District students, faculty, and staff and to any other individuals granted use of District information resources. This regulation shall be made available to users of District's Information Resources. This regulation shall not be construed as a waiver of any rights of Rancho Santiago Community College District; nor shall the intention be that it conflicts with applicable federal, state, and local laws.

2.0 Information Resources Applicability

This regulation refers to all District information resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and computer communication facilities owned, leased, operated, or contracted by the District. This includes, but is not limited to, personal computers, workstations and associated peripherals, servers, network infrastructure, mobile phones, mobile computing devices, software and all other information resources, regardless of whether used for administration, research, teaching, or other purposes.

3.0 Rights and Privileges

The District information resources are the sole property of Rancho Santiago Community College District. The District information resources are for District instructional and work-related purposes only.

The District reserves all rights, including termination of all access to information resources that it owns and operates. Access and privileges to RSCCD information resources are assigned and managed by Information Technology Services (ITS) as well as other systems administrators of individual information resources. Users may be authorized to use information resources and be granted appropriate access and

privileges following the approval steps prescribed for specific information resources. Users may not, under any circumstances, transfer or confer these privileges to other individuals.

4.0 Responsibilities

Anyone who uses the District's information resources to harass, or make defamatory remarks, shall bear full responsibility for his or her actions. District's information resources provide access to external networks, including those of public and private sources, which furnish electronic mail, information services, bulletin boards, websites, social media, etc. Users may encounter material that may be considered offensive or objectionable in nature or content. Users shall not transmit or store any illegal, fraudulent, malicious, harassing, or obscene communications and/or content that is encountered. District does not assume responsibility for the contents of any external information resource. District's role in managing these information resources is only as an information carrier. Users of District's information resources must comply with the acceptable use guidelines for external information resources accessed through District's information resources.

Users of District's information resources must never use any information resources to perform an illegal or malicious act. Any user attempting to change in any way the scope of information resource access to which they are authorized shall be regarded as malicious.

Users must not release any individual's (student, faculty or staff) personal information to anyone without proper authorization.

Users of District's information resources must not use such resources in a way that violates federal, state, local or other law, or in a way that violates any District policies.

5.0 Copyrights and Licenses

Users of District's information resources must respect copyrights and licenses to software and other on-line information. Information resources protected by copyright are not to be duplicated in any form, except as permitted by law or by written contract or with permission from the owner or legal holder of the copyright. Protected software may not be copied into, from, or by any District facility or system, except pursuant to a valid license or as otherwise permitted by copyright law. District may require written documentation verifying the user's right to make use of copyrighted materials prior to allowing them to be placed within District's information resources.

In addition to software, all other copyrighted information (text, images, icons, programs, etc.) retrieved from information resources must be used in conformance with applicable copyright and other law. Copied material must be properly attributed. Plagiarism of computer information is prohibited in the same way that plagiarism of any other protected work is prohibited.

6.0 Number of Simultaneous Users

The number and distribution of copied material must be handled in such a way that the number of simultaneous users in a department does not exceed the number of original copies purchased by that department, unless otherwise stipulated in the purchase contract.

7.0 Integrity of Information Resources

Users of District information resources must respect the integrity of computer-based information resources. No user shall attempt to deliberately degrade the performance of a District information resource.

Telecommunication rooms and facilities, where technology hardware is in operation, are environmentally conditioned to support optimal system performance. Construction activities that generate dust or debris, improper storage of items that affect airflow, or practices that impede access to this hardware are prohibited, as they are detrimental and may cause system failures, reduce system availability, or shorten the lifespan of the equipment. Users with access to these locations must exercise care to prevent damage or disruption to these information resources and must ensure that contractors or other individuals working in these areas understand and abide by these rules. Any construction or activity that may impede the proper functioning of the equipment in these areas must be coordinated with Information Technology Services.

8.0 Modification or Removal of Equipment

Users of District information resources must not attempt to modify or remove computer equipment, software, or peripherals that are owned by others without proper authorization.

9.0 Unauthorized Use

Users of District Information resources must not interfere with others' access and use of the District computers. This includes, but is not limited to: the sending of chain letters or excessive messages, either locally or off-campus; printing excess copies of documents, files, data, or programs; running grossly inefficient software when efficient alternatives are known by the user to be available; unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up a District computer or network; and damaging or vandalizing District computing facilities, equipment, software or computer files.

10.0 Unauthorized Programs

Users of District information resources must not intentionally develop or use programs which disrupt other users of District information resources or which access private or restricted portions of the system, or which damage the software or hardware components of the system. Users of District information resources must ensure that they do not use programs or utilities that interfere with other users of District information resources or that modify normally protected or restricted portions of the system or user accounts. If any unauthorized program(s) is(are) discovered on District resources, the District reserves the right to immediately remove or block access from the system in violation. The use of any unauthorized or destructive program will result in disciplinary action as provided in this procedure and may further lead to civil or criminal legal proceedings.

11.0 Unauthorized Access

Users of District information resources must not seek to gain unauthorized access to information resources and must not assist any other persons to gain unauthorized access.

12.0 Abuse of Computing Privileges

Users of District information resources must not access computers, computer software, computer data, or information, or networks without proper authorization, or intentionally

enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the District. For example, abuse of the networks to which the District belongs or the computers at other sites connected to those networks will be treated as an abuse of District computing privileges.

13.0 Reporting Problems

Any defects discovered in system accounting or system security must be reported promptly to the Information Technology Services (ITS) Help Desk so that steps can be taken to investigate and solve the problem.

14.0 Accounts and Password Protection

Users of District information resources are responsible for the proper use of individual accounts, including but not limited to, proper password protection. A computer user who has been authorized to use a password-protected account may be subject to both civil and criminal liability if the user discloses the password or otherwise makes the account available to others without permission of the system administrator.

Any user account that has been identified as compromised (meaning that an unauthorized individual has gained access to the user account) is subject to temporary suspension or deletion until the assigned account user can be validated and appropriate security remediation has been completed.

15.0 Usage

Computer users must respect the rights of other computer users. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to another person's information are a violation of District procedure and may violate applicable law.

16.0 Electronic Messaging Systems

The District has multiple electronic messaging systems, including but not limited to, an electronic mail (e-mail) system, instant messaging (IM) and text messaging platforms, messaging utilities within its Learning Management System and multiple other systems that allow messages to be delivered electronically (Electronic Messaging Systems).

Users are responsible for using these technologies responsibly and within the following policies:

- The District's Electronic Messaging Systems are not to be used to send defamatory, fraudulent, harassing, obscene, threatening, or other messages that intentionally embarrass, disparage or disrespect others and their opinions, violate applicable federal, state or other law, violate the District Code of Ethics (Board Policy 7701), Civility policy (Board Policy 7002), the Standards of Student Conduct (Board Policy 5500) or any other District policy, or which constitute the unauthorized release of confidential information.
- The District's Electronic Messaging Systems may not be used to transmit commercial or personal advertisements, solicitations or promotions.
- Sending unsolicited messages is prohibited, including the sending of junk mail or other advertising material to individuals who did not specifically request such material.
- Creating or forwarding chain letters or pyramid schemes of any type is prohibited.
- The District's Electronic Messaging Systems must not be used to create any messages that may be considered offensive or disruptive. Examples of messages deemed to be offensive are any which contain sexual implications, racial slurs, gender-specific comments or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin, gender, gender identity, gender expression, race or ethnicity, color, medical condition, genetic information, ancestry, marital status, physical or mental disability, pregnancy, or military and veteran status.
- Falsifying e-mail headers or routing information so as to obscure the origins of the e-mail or identity of the sender is a violation of this Administrative Regulation.
- Unauthorized access to others' e-mail accounts is prohibited.

- Personally identifiable information must not be e-mailed without encryption.
- Caution must be used when opening e-mail attachments or following hypertext links received from unknown senders, which may contain malware or viral code.
- Any e-mail or message found to contain malware, viral code or categorized as a phishing type message is subject to administrative removal without the consent of the user.
- While every reasonable attempt will be made to ensure the privacy of user accounts and electronic mail, users understand that there is no guarantee that accounts or electronic mail are private. Electronic mail is not 100% secure, nor is it delivered via a 100% secure information resource.
- Users understand that the District email system contains a set of technical tools to protect the security of its data. These tools allow technical staff to manage and secure smart phones and tablets when an email app is used to synchronize District issued email from them. The District uses these technical tools as required to protect the security of its information resources, in accordance with this regulation and as required by District policies and governing law. Users who choose to use an email app to synchronize their District issued email from a personally owned mobile smart phone or tablet may receive a "remote security administration" notification, a request to "allow my organization to manage my device," or a similar message prior to connecting to the District email system. These notifications indicate the presence of the technical tools previously mentioned and how they can potentially be used. However, the District only uses a limited set of standards to ensure basic email security on personally owned devices as a more specifically defined in:
  https://intranet.rsccd.edu/ITS/Pages/EmailMobileDevices.aspx
  The District is not able to see phone records, text messages, pictures, browsing history or any personal data stored or sent on personally owned devices and the District will not perform a remote device wipe on personally owned devices unless requested by the device owner. Users agree to allow these technical controls be implemented on their personally owned devices by their choice to synchronize email on them. Users understand that this type of usage is completely voluntary and not required by the District.

17.0 Generative Artificial Intelligence

Generative Artificial Intelligence (AI) is technology that can generate text, images, or other media in response to prompts and may be implemented through web applications, chatbot systems and other mechanisms. Users may only use Generative AI in a lawful, ethical manner that complies with all federal, state, or local laws and that does not violate any District policies or standards of academic integrity. Users shall not include personally identifiable information or other confidential data in their prompts when using Generative AI in order to maintain data privacy.

18.0 Information Belonging to Others

Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users, without the permission of those other users.

19.0 User Identification

Users shall not send communications or messages anonymously or without accurately identifying the originating account or station. However, systems that allow anonymous messaging to protect the identity of the sender are excluded from this provision.

20.0 Political, Personal, and Commercial Use

The District is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state and local laws regarding sources of income, political activities, use of property and similar matters.

20.1 Political Use

District information resources must not be used for partisan political activities where prohibited by federal, state, or other applicable laws.

20.2 Personal Use

District information resources given to users are provided to assist district employees and volunteers in the performance of their jobs and are intended for business and instructional use. Users are expected to exercise good judgment regarding the reasonableness of personal use of District information resources and assets. Personal use of District information resources and assets should be purely incidental. Incidental personal use should not conflict in any way with business objectives or interests, organizational values, or standards of business conduct.

20.3 Commercial Use

District information resources must not be used for commercial purposes. Users also are reminded that the ".cc" and ".edu" domains on the Internet have rules restricting or prohibiting commercial use, and users may not conduct activities not authorized within those domains.

21.0 Nondiscrimination

All users have the right to be free from any conduct connected with the use of Rancho Santiago Community College District information resources which discriminates against any person on the basis of national origin, religion, age, gender, gender identity, gender expression, race or ethnicity, color, medical condition, genetic information, ancestry, sexual orientation, marital status, physical or mental disability, pregnancy, or military and veteran status, or because he or she is perceived to have one or more of the foregoing characteristics, or based on association with a person or group with one or more of these actual or perceived characteristics. No user shall use the District network and computer resources to transmit any message, create any communication of any kind, or store information which violates any District regulation regarding discrimination or harassment, or which is defamatory or obscene, or which constitutes the unauthorized release of confidential information.

22.0 Computing Standards

The District maintains a list of approved computing standards, which is located here: https://rsccd.edu/Departments/Educational-Services/Technology-Advisor-Group/Pages/default.aspx

Computing Standards have been vetted to ensure compliance with the accessibility requirements of Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. §794d), and its implementing regulations set forth at Title 36, Code of Federal Regulations, Part 1194. Computing standards have also been assessed to ensure information security compliance and software compatibility across District technology platforms. District will only procure information resources within established computing standards. Use of information resources outside of computing standards cannot be guaranteed to satisfy accessibility and information security regulations. As such, exceptions may be prohibited and shall be reviewed by Information Technology Services

on a case-by-case basis. These computing standards are applicable to technology procured by the District and not to personally owned devices.

23.0 Disclosure

23.1 No Expectation of Privacy

The District Reserves the right to monitor all use of the District information resources and access all content stored in its systems to troubleshoot system problems, disruptions or outages and to assure compliance with these policies. Suspected inappropriate use of systems by individuals may also be investigated in order to protect the organization. Users should be aware that they have no expectation of privacy in the use of the District information resources or in anything they store, create, send, or receive on a District information resource. The District will exercise this right only for legitimate District purposes, including but not limited to ensuring compliance with this regulation and the integrity and security of its systems or as allowed by law.

23.2 Possibility of Disclosure

Users must be aware of the possibility of unintended disclosure of communications.

23.3 Retrieval

It is possible for information entered on or transmitted via computer and communications systems to be retrieved, even if a user has deleted such information.

23.4 Public Records

The California Public Records Act (Government Code Sections 6250 et seq.) includes computer transmissions in the definition of “public record” and nonexempt communications made on the District information resources must be disclosed if requested by a member of the public.

23.5 Litigation

Computer transmissions and electronically stored information may be discoverable in litigation.

Student files are considered educational records as covered by the Family Educational Rights and Privacy Act of 1974 (Title 20, Section 1232(g) of the United States Code). Such records are considered confidential under the law, but student files and electronic mail may be subject to search under court order if such files are suspected of containing information that could be used as evidence in a court of law. In addition, system administrators may monitor network traffic and/or access student files or electronic mail as required to protect the integrity of information resources (e.g., examining files or accounts that are suspected of unauthorized use or misuse, or that have been corrupted or damaged).

24.0 Title IV Information Security Compliance

The Gramm-Leach-Bliley Act requires entities that participate in Title IV Educational Assistance Programs to develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to the entity’s size and complexity. As a participating entity, the District has adopted Board Policy 3730 Information Security – Logging and Monitoring and associated Administrative Regulations to guide its information security program. Users of District information resources shall become familiar with Board Policy 3730 and its associated

Administrative Regulations as they provide further guidance on acceptable use of District information resources.

25.0 Violations

Users' information resources privileges may be suspended upon the discovery of violation of this regulation. Violations of this regulation will be dealt with in the same manner as violations of other District policies and regulations and may result in disciplinary review. In such a review, and as specified in the District's Board Policies and Administrative Regulations, the full range of disciplinary actions is available including the permanent loss of information resource use privileges, dismissal from the District, and legal action. Violations of these policies may constitute a criminal offense and may be prosecuted under applicable federal, state, and local law.

Those detecting violations of this Administrative Regulation must report the violation to their direct manager immediately, who will verify the nature of the violation and report it to the Information Technology Services (ITS) Help Desk and/or Human Resources and/or Admissions and Records, as appropriate.

26.0 Dissemination and User Acknowledgement

All users of District information resources shall be provided copies of the procedures and be directed to familiarize themselves with them. All users must review and acknowledge their understanding of these procedures on a regular basis. Human Resources (HR) will provide the Administrative Regulation and acknowledgement links to new staff upon hire. Admissions and Records will provide the Administrative Regulation and acknowledgement links to new students. Vendors and contractors will be provided a copy of these procedures in Purchase Orders and/or contract clauses.

A "pop-up" screen addressing appropriate portions of these procedures shall be installed on all applicable systems to inform existing students and staff, vendors, guests and other users. The "pop-up" screen shall appear prior to accessing applicable systems. Continued usage of these systems shall constitute users' continued acknowledgement and acceptance of compliance with these procedures. Students and staff shall sign and date the acknowledgement and waiver included in this in this regulation stating that they have read and understood this regulation and will comply with it. This acknowledgement and waiver shall be in the form as follows:

> ***Information Resources Acceptable Use Agreement*** *(sample language)*
> *I have received and read a copy of AR 3720 Information Resources Acceptable Use on (_____) and recognize and understand the guidelines. I agree to abide by the standards set in the procedures established in AR 3720 for the duration of my employment or enrollment. I am aware that violations of this Information Resources Acceptable Use AR may subject me to disciplinary action, including but not limited to revocation of my network account up to and including termination, expulsion and/or prosecution for violations of State or Federal law.*
>
> *Name:* _____
> *Employee or Student ID:* _____
> *Signature:* _____
> *Date:* _____

Responsible Manager: Assistant Vice Chancellor, Information Technology Services

Adopted: **August 11, 2014 (Previously AR 7000)**
Revised: **June 6, 2022**
Revised: **October 2, 2023**

STP Proposed Taskforce Membership:

	Santa Ana College	Santiago Canyon College	Noncredit	District
Students				N/A
Faculty	Jason Sims	Scott James	Jose Lopez Mercedes	N/A
Classified				Jeremy Collins
Administrators	John Steffens Marvin Gabut		Jennifer Hoeger	Jesse Gonzalez Dane Clacken Ron Gonzalves Kimberly Perna

LAPTOP – STAFF AND ADMIN (SPECIAL CASE)	
USE CASE – Special work specific cases	
CURRENT	**NEW**
Microsoft Surface Laptop 5	Microsoft Surface Laptop 6
	
District Cost: $2,200	District Cost: $1,899
Base Configuration: • Intel Processor i7-1255U • 16GB LPDDR5 • 512GB PCIe NVMe TLC SSD • 13.5” and 15” screen size • 15’’ FHD LED UWVA 1920x1080 Display • 17 hours • 4-year warranty	**Base Configuration:** • Intel Core Ultra 7 – 165H • 16GB LPDDR5 • 512GB Gen 4 SSD • 13.5” and 15” screen size • 15’’ PixelSense 2496 X 1664 Display • 19 hours battery life • 4-year warranty

LAPTOP / TABLET – STAFF AND ADMIN (SPECIAL CASE)	
USE CASE – Special work specific cases	
CURRENT	**NEW**
Microsoft Surface Pro 9	Microsoft Surface Pro 10
	
District Cost: $1,568	District Cost: $1,599
Base Configuration: • Intel Processor i7-1255U: 4 cores • 16GB LPDDR5 • 256GB SSD • Integrated HD 1080p Webcam • Dual Mic Array • 4-year Warranty • 15.5-hour battery life	**Base Configuration:** • Intel Core Ultra 7 – 165U • 16GB LPDDR5 • 256GB SSD • 1440p Quad HD Webcam • Dual Mic Array w/ voice focus • 4-year Warranty • 19-hour battery life

This Agreement for the purchase of certain "Goods and Services" is made by and between the Rancho Santiago Community College District (hereinafter "District"), a California community college district and political subdivision of the State of California, located at 2323 N. Broadway, Santa Ana, CA 92706, on behalf of the Admissions and Records Offices at Santa Ana College and Santiago Canyon College and CourseMaven, Inc. dba DualEnroll.com, a Corporation, having its principal place of business located at 43498 Butler Place, Leesburg, VA 20176 (hereinafter "Supplier").

1. Statement of Work

Supplier agrees to provide the Goods and/or Services as more fully described in Attachment A: Statement of Work, referencing this Agreement number, and any and all incorporated documents at the prices set forth herein. District is not obligated to purchase a minimum amount of Goods and/or Services from Supplier. Nothing in the Statement of Work will be construed to prevent District from entering into similar agreements with any third parties, including, without limitation, other parties that may be in competition with Supplier.

2. Term

The term of the Agreement shall be in accordance with the applicable Statement of Work referencing this Agreement number and is subject to earlier termination as provided below. This Agreement may be extended upon the mutual written agreement of the parties.

3. Purchase Order

Unless otherwise provided in this Agreement, Supplier may not begin providing Goods and/or Services, including access or licenses, until District approves a Purchase Order for said Goods and/or Services. District does not make payments in advance of the completion of delivery of Goods and Services.

4. Invoices

Supplier shall be required to submit an invoice in accordance with Section 3 of the General Terms and Conditions to AP@RSCCD.edu.

All payment terms shall be Net 30.

5. Notices

In accordance with Article 16 of the General Terms and Conditions, notices shall be given by personal service or overnight courier service or by U.S. Mail, mailed either by certified or registered mail, return receipt requested, with postage prepaid to the addresses specified below.

To District, regarding all matters, to the address below:

Name	ATTENTION: VICE CHANCELLOR OF BUSINESS SERVICES
Office	Rancho Santiago Community College District
Address	2323 N. Broadway, Santa Ana, CA 92706

With a copy to the applicable College Vice President or Assistant Vice Chancellor:

Name & Title	Dr. Jeffrey Lamb, Vice President of Academic Affairs
Department and College	Academic Affairs, Santa Ana College
Address	1530 W. 17th. St. Santa Ana, CA 92706

With a copy to the applicable College Vice President or Assistant Vice Chancellor:

Name & Title	Dr. Jason Parks, Vice President of Academic Affairs
Department and College	Academic Affairs, Santiago Canyon College
Address	8045 E. Chapman Ave., Orange, CA 92869

With a copy to the applicable Department Administrators:

Name & Title	Matt Valerius, Associate Dean of Career Education and Dual Enrollment
Department and College	Office of Career Education and Dual Enrollment, Santa Ana College
Phone	(714) 564-6382
Email	Valerius_Matthew@sac.edu
Address	1530 W. 17th. St. Santa Ana, CA 92706

Name & Title	Tuyen Nguyen, Associate Dean
Department and College	Admissions and Records, Santiago Canyon College
Phone	(714) 628-4844
Email	Nguyen_tuyen@sccollege.edu
Address	8045 E. Chapman Ave., Orange, CA 92869

For matters related to breach of Data Protection Exhibit, send a copy to

Name	ATTENTION: Assistant Vice Chancellor, Information Technology Services
Office	Rancho Santiago Community College District
Address	2323 N. Broadway, Santa Ana, CA 92706

To Supplier:

Name & Title	Janet Van Pelt, Founder & CEO
Company	DualEnroll.com
Phone	(703) 884-9131 ext. 523
Email	jvanpelt@dualenroll.com
Address	43498 Butler Place, Leesburg, VA 20176

6. Federal Funding

Are federal and/or state funds being utilized for this Agreement? ☒ Yes

7. Follow-on Restriction

If the Goods and/or Services involve consulting services, Supplier understands and agrees that Supplier cannot later be considered for any contract work to perform "required, suggested, or otherwise deemed appropriate" service flowing out of the consulting services performed pursuant to this Agreement.

8. Insurance

Supplier shall deliver the PDF version of the Certificate of Insurance and all additional insured endorsements to Purchasing Services at purchasing@rsccd.edu by email with the following text in the subject field: CERTIFICATE OF INSURANCE – COURSEMAVEN, INC. DVA DUALENROLL.COM.

9. Record Keeping

Records created pursuant to the Agreement that contain personal information about individuals (including statements made by or about individuals) may become subject to the California Information Practices Act of 1977 (Civil Code §§ 1798 through 1798.78), which includes a right of access by the subject individual. While ownership of confidential or personal information about individuals is subject to negotiated agreement between District and Supplier, records will normally become District's property, and subject to state law and District policies governing privacy and access to files. When collecting the information, Supplier must inform the individual that the record is being made, and the purpose of the record. Use of recording devices in discussions with employees is permitted only as specified in the Statement of Work.

10. Incorporated Documents

The following documents are incorporated and made a part of the Agreement by reference as if fully set forth herein, listed in the order of precedence following the Agreement:

- Attachment A Statement of Work
- Attachment B General Terms and Conditions, dated November 9, 2023, as modified.
- Data Protection Exhibit
- Service Level Agreement Exhibit
- Other (specify): CourseMaven Master Services Agreement dated June 4, 2024.

General Purchase Terms and Conditions can be found here:
https://www.rsccd.edu/Departments/BusinessServices/Documents/General%20Purchase%20Terms%20and%20Conditions%20V1_11092024.pdf

11. Entire Agreement

This Agreement, including all incorporated documents, contain the entire agreement between the parties and supersede all prior written or oral communications or agreements with respect to the subject matter herein.

The Agreement is signed below by the parties' duly authorized representatives.

RANCHO SANTIAGO COMMUNITY COLLEGE DISTRICT	CourseMaven, Inc. dba DualEnroll.com
_____	_____
Signature Date	Signature of Supplier Date
_____	_____
Name, Title	Name, Title

ATTACHMENT A: STATEMENT OF WORK

This Statement of Work ("SOW") is issued pursuant to Purchase Agreement or Bid Number #N/A dated August 15, 2024 between District and Supplier ("Agreement").

1. Term of SOW

This SOW will begin on September 1, 2024 ("Effective Date") and continue through August 31, 2025 ("Expiry Date"). This SOW may not be renewed or otherwise amended except as set forth in the Agreement.

2. Description of Goods and/or Services and Completion Timeframe

Line Item	Deliverables	Description	Cost
1	DualEnroll.com RSCCD Implementation	Supplier will work with Admissions and Records Offices at SAC and SCC, as well as District ITS, to configure and test the DualEnroll.com software platform.	$30,000
2	DualEnroll.com annual software license (Registration module)	Supplier will provide SAC and SCC an annual software license for the Registration module that includes an unlimited number of users for each college (including access by high school partners and students).	$45,044

3. Pricing, Invoicing Method, and Settlement Method and Terms

Pricing is addressed below.

a) "Fixed Price Services" to be rendered under this SOW, including Goods and/or Services to be provided as part of Fixed Price Services, are described in this section as: $75,044.

4. District Obligations

District and college staff will be responsible for assisting DualEnroll.com with configuring the software to meet the needs of each college's Admissions and Records Office, including with attending regular implementation meetings, providing information on current enrollment processes and workflows, assisting with setting up API connections as needed, and testing the software's functionality within each college's processes to troubleshoot issues and make corrections as needed.

5. Place(s) of Performance

Services will be delivered remotely from outside California.

6. Key Personnel

Supplier's Account Manager is listed below, is subject to District approval, and has overall responsibility for managing the District/Supplier relationship:

Name & Title	Janet Van Pelt, Founder & CEO
Company	DualEnroll.com
Phone	(703) 884-9131 ext. 523

Email	jvanpelt@dualenroll.com
Address	Enter Supplier address.

Subcontractors authorized to provide Goods and/or Services under this SOW:

Name of Subcontractor	Goods and/or Services the Subcontractor will provide
N/A	N/A

The District's contact, responsible for acceptance/rejection of project results/deliverables, is:

Name & Title	Mark DeAsis, Dean of Enrollment & Support Services
College & Department	Admissions and Records, Santa Ana College
Phone	(714) 564-6040
Email	deasis_mark@sac.edu
Address	1530 W. 17th. St. Santa Ana, CA 92706

Name & Title	Tuyen Nguyen, Associate Dean of Admissions and Records
College & Department	Admissions and Records, Santiago Canyon College
Phone	(714) 628-4844
Email	Nguyen_tuyen@sccollege.edu
Address	8045 E. Chapman Ave., Orange, CA 92869

7. Acceptance Criteria and Testing

The Supplier will work with the Admissions and Records Offices at Santa Ana College and Santiago Canyon College in configuring and testing the software implementation to ensure the product will support the needs of each college with streamlining the enrollment process for high school students taking college courses. In particular, the following functionality must work to the satisfaction of each college's Admissions and Records Team:

a. Enabling Students, parents, and high school staff to initiate and complete the required steps in the enrollment process in an organized and user-friendly way;
b. Ensuring students have valid applications and meet course-level requirements prior to registration;
c. Sending automated communication and notifications via emails and/or text messages to relevant stakeholders when action is required;
d. Gathering permissions from parents and high school staff, as required prior to clearing students to register;
e. Creating electronic copies of required permission forms that can be archived by each college;
f. Flagging students from specific high schools and setting up course- and/or section-level registration restrictions;
g. Incorporating course- and section-level information from the colleges' semester course offerings that will enable students to self-register;
h. Generating automated confirmation emails and/or text messages once students have successfully completed all required steps; and
i. Keeping an audit trail of all registration activity for 7 years.

8. Changes to the Statement of Work

District may desire to change the Goods and/or Services following execution of this SOW. If so, District will submit a written Amendment to Supplier describing the changes in appropriate detail. If an Amendment does not require Supplier to incur any additional material costs or expenses, then Supplier will make the modification within ten (10) business days of Supplier's receipt of District's Amendment. If an Amendment does require that Supplier incur additional material costs or expenses, then Supplier in good faith will provide District with a written, non-binding assessment of the costs and expenses and the time required to perform the modifications required by the Amendment, within ten (10) business days of Supplier's receipt of District's Amendment. District will notify Supplier in writing within ten (10) business days after receipt of Supplier's response to the Amendment as to whether District accepts Supplier's assessment of the costs, expenses, and timeline for completion. After written acceptance by the District and approval of the Amendment by the District's Board of Trustees, District will compensate Supplier for implementation of an Amendment in accordance with the terms and conditions of the relevant Amendment. All other terms and conditions of the Agreement shall remain in full force and effect.

---END STATEMENT OF WORK---

ATTACHMENT B

GENERAL PURCHASE TERMS AND CONDITIONS

ARTICLE 1. GENERAL

The equipment, materials, supplies ("Goods"), services ("Services") and/or licenses ("Licenses") furnished by Supplier (together, the "Goods and Services") and covered by the District's Purchase Agreement ("Purchase Agreement"), Purchase Order ("PO") and/or other agreement (which, when combined with these Terms and Conditions and any other documents incorporated by reference, will constitute the "Agreement") are governed by the terms and conditions set forth herein. As used herein, the term "Supplier" includes Supplier and its sub-suppliers at any tier. As used herein, "District" refers to the Rancho Santiago Community College District or Rancho Santiago Community College District on behalf of Santa Ana College or Santiago Canyon College (hereinafter the "Colleges") identified in the Agreement and/or the PO. District and Supplier individually will be referred to as "Party" and collectively as "Parties." Any defined terms not defined in these General Purchase Terms and Conditions will have the meaning ascribed to such term in any of the other documents incorporated in and constituting the Agreement. No other terms or conditions will be binding upon the Parties unless accepted by them in writing. Supplier accepts all of the Agreement's terms and conditions either in writing, by shipping any portion of the Goods, or performing any portion of the Services, or issuing access to any portion of a License. The terms of any proposal referred to in the Agreement are included and made a part of the Agreement only to the extent the proposal specifies the Goods and/or Services ordered, the price therefor, and the delivery thereof, and then only to the extent that such terms are consistent with the terms and conditions of the Agreement. No Agreement shall be binding on the District until ratified or approved by the District's Board of Trustees.

ARTICLE 2. TERM AND TERMINATION

A. As applicable, the term of the Agreement ("Initial Term") will be stated in the Agreement. Following the Initial Term, the Agreement may be extended by written mutual agreement and approved by the District's Board of Trustees but under no circumstance will the term of the Agreement, whether the Initial Term or by extension, exceed five (5) years in accordance with Education Code section 81644.

B. District may, by written notice stating the extent and effective date thereof, terminate the Agreement for convenience in whole or in part, at any time. The effective date of such termination shall be consistent with any requirements for providing notice specified in the Agreement, or immediate if no such terms are set forth in the Agreement.

C. District may by written notice terminate the Agreement for Supplier's breach of the Agreement, in whole or in part, at any time, if Supplier refuses or fails to comply with the provisions of the

Agreement, or so fails to make progress as to endanger performance and does not cure such failure within fifteen (15) days,. In such an event, District may purchase or otherwise secure Goods and/or Services.

D. In the event that Supplier files for protection under bankruptcy laws, makes an assignment for the benefit of creditors, appoints or suffers appointment of a receiver or trustee over its property, files a petition under any bankruptcy or insolvency act or has any such petition filed against it which is not discharged within thirty (30) days of the filing thereof, then District may terminate this Agreement effective immediately upon written notice to Supplier.

E. District reserves the right to immediately terminate or otherwise suspend this Agreement without notice if District's Board of Trustees determines that funding for the Services is insufficient.

ARTICLE 3. PAYMENT

Pricing is set forth in the Agreement or PO, and the amount District is charged and responsible for shall not exceed the amount specified in the Agreement without prior written approval in accordance with the terms of the Agreement. District will pay Supplier, upon submission of acceptable invoices, for Goods and Services provided and accepted. Invoices must be itemized and reference the Agreement or PO number. Supplier shall submit detailed billing information not more than once per month, and, if applicable, District-authorized expenses incurred during the billing period. Any invoices must include:

1. Invoice date;
2. Date(s) of service(s) and/or description, quantity, catalog number, and manufacturer number of the item ordered;
3. District's Purchase Order number;
4. Net cost of each item;
5. Any pay/earned/dynamic discount;
6. If applicable, the associated Agreement number;
7. Reference to the original order number for all credit memos issued; and
8. Supplier's taxpayer Identification Number.

Payment terms are Net 30 for Goods and Services accepted pursuant to the Agreement. District will not pay shipping, packaging, or handling expenses, unless specified in the Agreement or PO. Unless otherwise provided, freight is to be FOB destination. Any of Supplier's expenses that District agrees to reimburse will be reimbursed under the District's Travel Policy in accordance with Board Policy 7400 and Administrative Regulation 7400 found at https://rsccd.edu/Trustees/Documents/ARs/ARs-Chapter%207/AR%207400%20Travel.pdf. Where applicable, Supplier will pay all taxes imposed on Supplier in connection with its performance under the Agreement, including any federal, state, and local income, sales, use, excise and other taxes or assessments. Notwithstanding any other provision to the contrary, District will not be responsible for any fees, interest or surcharges Supplier wishes to impose. The District is exempt from federal excise taxes.

ARTICLE 4. INSPECTION AND ACCEPTANCE

The Goods and/or Services furnished will be exactly as specified in the Agreement, free from all defects in Supplier's performance, design, skill, and materials, and, except as otherwise provided in the Agreement, will be subject to inspection and testing by District at all times and places. If, prior to final acceptance, any Goods and/or Services furnished are found to be incomplete, or not as specified, District may reject them, require Supplier to correct them at the sole cost of Supplier, or require provision of such Goods and/or Services at a reduction in price that is equitable under the circumstances. If Supplier is unable or refuses to correct such deficiencies within a time District deems reasonable, District may terminate the Agreement in whole or in part.

ARTICLE 5. INTELLECTUAL PROPERTY AND DATA RIGHTS

A. Should the Goods and/or Services become, or in Supplier's opinion be likely to become, the subject of a claim of infringement of any patent, copyright, trademark, trade name, trade secret, or other proprietary or contractual right of any third party, Supplier will provide written notice to District of the circumstances giving rise to such claim or likely claim. In the event that District receives notice of a claim of infringement or is made a party to or is threatened with being made a party to any claim of infringement related to the Goods and/or Services, District will provide Supplier with notice of such claim or threat. Supplier shall fully indemnify and defend the District from any such claims covered in this paragraph. Following receipt of such notice, Supplier will either (at Supplier's sole election) (i) procure for District the right to continue to use the affected portion of the Goods and/or Services, or (ii) replace or otherwise modify the affected portion of the Goods and/or Services to make them non-infringing, or (iii) obtain a reasonable substitute product for the affected portion of the Goods and/or Services, provided that any replacement, modification or substitution under this paragraph does not effect a material change in the Goods and/or Services' functionality. If none of the foregoing options is reasonably acceptable to District, District will have the right to terminate the Agreement without damage, penalty, cost or further obligation.

B. District Information shall belong exclusively to District and unless expressly provided, this Agreement shall not be construed as conferring on Supplier any patent, copyright, trademark, license right or trade secret owned or obtained by District. Any right for Supplier to use District Information is solely provided on a non-exclusive basis, and only to the extent required for Supplier to provide the Goods or Services under the Agreement. As used herein, "District Information" means any information

or data created, received, and/or collected by District or on its behalf, including but not limited to application logs, metadata and data derived from such data.

C. Supplier will not use the District name, abbreviation of the District name, trade names and/or trademarks (i.e., logos and seals) or any derivation thereof, in any form or manner in advertisements, reports, or other information released to the public, or place the District name, abbreviations, trade names and/or trademarks or any derivation thereof on any consumer goods, products, or services for sale or distribution to the public, without District's prior written approval. Supplier agrees to comply, at all times, with California Education Code Section 72000, subsection (b)(4). District will, upon its approval, will furnish Supplier with camera-ready artwork for such use. District may limit or otherwise place conditions on Supplier's use of District's name and/or logos in which case such limitations will be incorporated in this Agreement. Supplier agrees to not revise, change, or otherwise alter any material related to District's name and/or logo without District's prior written consent.

ARTICLE 6. INDEMNITY AND LIABILITY

B. To the fullest extent allowed by law, Supplier shall indemnify, defend, and hold harmless District, its Board, officers, agents, and employees ("Indemnitees") from any and all, actual and alleged, claims, demands, suits, actions, proceedings, loss, cost, and damages, including attorney's fees and/or litigation expenses, which may be brought or made against or incurred on account of breach, or loss of or damage to any property, or for injuries to or death of any person, or financial loss incurred by Indemnitees, caused by, arising out of, or contributed to, in whole or in part, by reasons of any negligent act, omission, professional error, fault, or mistake of Supplier, its employees, agents, representatives, or subcontractors, their employees, agents, or representatives in connection with or incident to the performance of or founded upon the Agreement, or arising out of Workers Compensation claims, Unemployment Compensation claims, or Unemployment Disability Compensation claims of employees of Supplier and/or its subcontractors of claims under similar such laws and obligations. Supplier's obligation under this provision shall not extend to any liability caused in whole or in part by the any negligent action, omission, , willful misconduct or unlawful acts of any employee, agent or affiliate of the District. Such indemnification shall specifically include infringement claims made against any and all intellectual property supplied by Supplier and third-party infringement under the Agreement. Notwithstanding the foregoing, in no event shall either party be liable for any incidental, indirect, special, consequential or punitive damages, regardless of the nature of the claim, including, without limitation, lost profits, costs of delay, any failure of delivery, business interruption, costs of lost or damaged data or documentation or liabilities to third parties arising from any source, even if advised of the possibility of such damages.

B. Indemnification Process: The party seeking indemnification hereunder ("**Indemnified Party**") shall promptly inform the other party ("**Indemnifying Party**") of any suit or proceeding filed against the Indemnified Party for which the Indemnified Party is entitled to indemnification hereunder. The Indemnifying Party may direct the defense and settlement of any such claim, with counsel of its choosing. The Indemnified Party will provide the Indemnifying Party, at the Indemnifying Party's expense, with information and assistance reasonably necessary for the defense and settlement of the claim. The Indemnified Party shall have the right, but not the obligation, at its sole expense to participate in (but not to control) the defense of any such suit or proceeding.

Supplier shall reimburse or otherwise be responsible for any costs, fines or penalties imposed against District as a result of Supplier's Breach of District Information and/or failure to cooperate with District's response to such Breach. As used herein, "Breach" means:

a. Any disclosure of District Information to an unauthorized party or in an unlawful manner not caused in whole or in part by action or omission of the District, its employees, agents or affiliates;
b. Unauthorized or unlawful acquisition of information that compromises the security, confidentiality, or integrity of District Information and/or IT Resources not caused in whole or in part by action or omission of the District, its employees, agents or affiliates.

"IT Resources" means IT infrastructure, cloud services, software, and/or hardware with computing and/or networking capability that is Supplier owned/managed

ARTICLE 7. INSURANCE

A. Supplier (and all subcontractors) agrees to maintain, in full force and effect, at Supplier's expense, the following insurance coverage from an admitted carrier in the State of California with an AM Best Rating of A-VII or higher:

1. Commercial General Liability insurance, with limits of not less than One Million Dollars ($1,000,000) per occurrence / Two Million Dollars ($2,000,000) aggregate and must include coverage for property damage, bodily injury, personal & advertising injury, products and completed operations, liability assumed under an insured contract (including tort of another assumed in a business contract), and independent contractor's liability, written on an "occurrence" form;
2. Workers' Compensation insurance. This coverage is required unless Supplier provides written verification it has no employees.
3. Errors and Omissions/Professional Liability: (If applicable) For financial loss or harm caused to the District that arise out of Supplier's negligence $1,000,000 per occurrence / $1,000,000 annual aggregate.
4. Cyber Liability: (If applicable) For financial loss or harm caused to the District that arises out of loss or theft of data, breach of data, disruption of networks, intrusion of virus, malware, disclosure of private information, notification, credit monitoring, breach response costs, regulatory fines and penalties, and infringement of intellectual property $2,000,000 per

occurrence / $2,000,000 annual aggregate.

B. Supplier agrees to:

1. Name District, District's Board of Trustees, its officers, agents, and employees as additional insured under its general liability and auto policy(ies);
2. Ensure that the Certificate(s) of Insurance shall provide thirty (30) days prior written notice of cancellation;
3. Ensure that Supplier's Insurance to be Primary and any insurance or self-insurance maintained by the District, its Board of Trustees, officials, employees, volunteers, and agents shall be excess of the Supplier's insurance and shall not contribute with it;
4. Deliver Certificate(s) of Insurance and Additional Insured Endorsement(s) evidencing the required coverages to the District, which shall be subject to the District approval for adequacy of protection. All certificates must be delivered before the Goods and Services are to commence. However, failure to obtain the required documents prior to the work beginning shall not waive the Supplier's obligation to provide them;
5. Hereby grant to District, its Board of Trustees, employees, volunteers, and agents a waiver of any right to subrogation which any insurer of said Supplier may acquire against the District, its Board of Trustees, officials, employees, volunteers, and agents by virtue of the payment of any loss under such insurance. Supplier shall obtain any endorsement that may be necessary to affect this waiver of subrogation, but this provision applies regardless of whether or not District, its Board of Trustees, officials, employees, volunteers, and agents have received a waiver of subrogation endorsement from the insurer.

An Umbrella Liability policy (or Excess Liability) may be used to provide additional Commercial General Liability, Automobile Liability, and Employers' Liability limits to meet District's minimum coverage requirements provided all requirements set forth herein are fully satisfied with respect to such policy. If Supplier maintains broader coverage and/or higher limits than the minimums required herein, District shall be entitled to the broader coverage and/or higher limits maintained by the Supplier.

C. If the Data Protection Exhibit is incorporated into this Agreement, or if the scope of this Agreement requires Supplier to develop a system, website, web or mobile application or other software technology for the District, Supplier shall maintain Cyber Liability Insurance, with limits not less than $2,000,000 per occurrence or claim, $2,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Supplier in this Agreement and shall include, but not be limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, disruption of networks, intrusion of virus(es), malware, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs, regulatory fines, penalties, as well as notification and credit monitoring expenses with limits sufficient to respond to these obligations. District, its Board of Trustees, employees, agents, and volunteers must be named as additional insureds with respect to liability arising out of work or operations performed by or on behalf of Supplier under this Agreement.

D. If the Data Protection Exhibit is incorporated into this Agreement, or if the scope of this Agreement requires Supplier to develop a system, website, web or mobile application or other

software technology for the District, Supplier shall maintain Technology Professional Liability (Errors and Omissions) Insurance appropriate to Supplier's profession, with limits not less than $2,000,000 per occurrence or claim, $2,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Supplier in this agreement and shall include, but not be limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, disruption of networks, intrusion of virus(es), malware, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs, regulatory fines, penalties as well as notification and credit monitoring expenses with limits sufficient to respond to these obligations. District, its Board of Trustees, employees, agents, and volunteers must be named as additional insureds with respect to liability arising out of work or operations performed by or on behalf of Supplier under this Agreement.

ARTICLE 8. CONFIDENTIALITY

A. Under the terms of this Agreement, Supplier may receive or obtain access to student data, pupil records, or other information that is privileged, confidential, not publicly available, which is covered by federal or state privacy laws, rules, and regulations, or which is otherwise considered confidential and protected from disclosure by the policies and procedures of District ("Confidential Information"). Without limiting the generality of the foregoing, "Confidential Information" shall be defined as any information which is (i) marked as "Confidential" at the time of disclosure; (ii) if disclosed orally, identified at the time of such oral disclosure as confidential, and reduced to writing as "Confidential" within thirty (30) das of such disclosure; and (iii) if not marked as "Confidential", information that would be considered by a reasonable person in the relevant field to be confidential given its content and the circumstances of its disclosure. Supplier understands and agrees that all Confidential Information shall be preserved and protected as privileged or confidential, that Confidential Information shall be held strictly in accordance with District's policies and procedures, that Confidential Information shall be preserved and held in compliance with all applicable state or federal laws, rules, or regulations, that Supplier will not access, use or disclose Confidential Information other than to carry out the purposes for such disclosure, and that Confidential Information shall not be shared with any third party without the expressed written authorization of District or as required by applicable law. Any such disclosure of Confidential Information by Supplier to its employees shall only be as is necessary for the performance of its obligations under this Agreement and employees receiving Confidential Information shall be informed of the obligations governing the access, use, and disclosure of Confidential Information prior to Supplier's disclosure. Supplier shall be liable for any breach of this Agreement by its employees and shall fully indemnify and defend the District and Indemnitees from any claims, liability, costs, or damages arising from or related to any such breach. For avoidance of doubt, this provision prohibits Supplier from using for its own benefit Confidential Information and any information derived therefrom. For the avoidance of doubt, the sale of Confidential Information is expressly prohibited.

B. Compliance with Applicable Laws and Industry Best Practices. Supplier agrees to comply with all applicable state and federal, laws, as well as industry best practices, governing the collection, access, use, disclosure, safeguarding and destruction of Confidential Information. Supplier agrees to protect the privacy and security of Confidential Information according to all applicable laws and industry best practices, and no less rigorously than it protects its own information, but in no case less than reasonable care.

C. Notwithstanding Supplier's obligation to hold Confidential Information and any information derived therefrom in strict confidence, information received from the District will not be considered confidential to the extent that: (i) Supplier can demonstrate by written records was known to Supplier prior to the effective date of the Agreement; (ii) is currently in, or in the future enters, the public domain other than through a breach of the Agreement or through other acts or omissions of Supplier; (iii) is obtained lawfully from a third party; or (iv) is disclosed under the California Public Records Act or legal process. For the avoidance of doubt, as applicable to Supplier's Services, Confidential Information may include any information that identifies or is capable of identifying a specific individual, including but not limited to:

1. Personally identifiable information,
2. Protected Health Information as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the HIPAA regulations (including, but not limited to 45 C.F.R. § 160.103),
3. Medical information as defined by California Civil Code § 56.05,
4. Cardholder data,
5. Student records not defined as directory information in District's Board Policy 5040, found here: https://rsccd.edu/Trustees/Documents/Board%20Policies/BPs-Chapter%205/BP%205040%20Student%20Records,%20Directory%20Information%20and%20Privacy.pdf, or
6. Individual information that is subject to laws restricting the use and disclosure of such information, including but not limited to.

    i. Article 1, Section 1 of the California Constitution; the California Information Practices Act (Civil Code § 1798 et seq.);
    ii. The federal Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801(b) and 6805(b)(2));
    iii. The federal Family Educational Rights and Privacy Act (20 U.S.C. § 1232g);
    iv. The federal Fair and Accurate Credit Transactions Act (15 U.S.C. § 1601 et seq.);
    v. The Fair Credit Reporting Act (15 U.S.C. § 1681 et seq), and
    vi. Applicable international privacy laws, including, but not limited to the General Data Protection Regulation.

D. If Supplier is required by a court of competent jurisdiction or an administrative body to disclose Confidential Information, Supplier will notify District in writing immediately upon receiving notice of such requirement and prior to any such disclosure (unless Supplier is prohibited by law from doing so), to give District an opportunity to oppose or otherwise respond to such disclosure. To the extent Supplier still required to disclose Confidential Information, Supplier will furnish only that portion that is legally required and will exercise all reasonable efforts to obtain reliable assurance that confidential treatment will be afforded to any Confidential Information.

E. Supplier's transmission, transportation or storage of Confidential Information outside the United States, or access of District Information from outside the United States, is prohibited except with prior written authorization by District.

F. Supplier acknowledges that for the purposes of this Agreement, if Supplier has access to non-directory student information as defined by District Board Policy 5040, found here, it is designated as a "school official" with a "legitimate educational interest" in the non-directory student information, as

those terms have been defined under the Family Educational Rights and Privacy Act (FERPA) and its implementing regulations at 34 CFR 99. Supplier acknowledges that non-directory student information is classified as Confidential Information and agrees to abide by the limitations and requirements imposed by 34 CFR 99.33 (a) on school officials and District Board Policy 5040. Supplier shall use the non-directory student information only for the purposes of fulfilling its duties under the Agreement and it will not monitor or share such data with or disclose it to any third party except as provided for in this Agreement, as required by law, or authorized in writing by District or subject student. By way of illustration and not of limitation, Supplier will not use such data for Supplier's own benefit and, in particular, will not engage in "data mining" of District's data or communications, whether through automated or human means, except as necessary to fulfill its duties under this Agreement, which includes providing and improving the Supplier's Goods and/or Services, as defined in this Agreement, or as specifically and expressly provided for in this Agreement, an Addendum, as required by law, or authorized in writing by District.

G. Supplier acknowledges that remedies at law would be inadequate to protect District against any actual or threatened breach of this Article by Supplier, and, without prejudice to any other rights and remedies otherwise available to District, Supplier agrees to the granting of injunctive relief in District's favor without proof of actual damages.

ARTICLE 9. EXPENSES

Supplier shall furnish at its own expense all necessary overhead, administrative and support services, equipment, clerical personnel, facilities, communications and related facilities and personnel necessary to provide the Goods, perform the Services, or issue its License. All fees and expenses for services of Supplier under this Agreement, and District's obligations to compensate Supplier for services, shall solely be governed by the Agreement. Should Supplier incur additional or unanticipated expenses, District shall not be obligated to pay for, or reimburse, said expenses to the extent such expenses are not included within the compensation specifications set forth in the Agreement. District shall be entitled, at its sole and unrestricted discretion, to refuse to amend this Agreement or to otherwise voluntarily pay such additional and unanticipated expenses.

ARTICLE 10. W-9

Supplier agrees to provide a completed "Request for Taxpayer Identification Number and Certification" (Form W-9) with this signed Agreement and understands that the District will report payment information to the Internal Revenue Service under the name and TIN or SSN, whichever is applicable, provided by Supplier.

ARTICLE 11. INTENTIONALLY LEFT BLANK

ARTICLE 12. PERMITS AND/OR LICENSES

If applicable, Supplier and all Supplier's employees or agents shall secure and maintain in force such permits and licenses as are required by law in connection with the Goods and Services pursuant to this Agreement.

ARTICLE 13. WARRANTIES

A. Supplier warrants that all Goods and Services provided in accordance with this Agreement shall be provided in a manner consistent with the standard of care, diligence, and skill ordinarily exercised by professionals in similar fields and circumstances in accordance with sound professional practices.

B. Supplier warrants that they have exercised commercially reasonable best efforts to ensure that the Goods and Services to be provided under this Agreement complies with the accessibility requirements of Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C §794d), and its implementing regulations set forth at Title 36, Code of Federal Regulations, Part 1194. Supplier has provided College with VPAT's describing the compliance of software products or services provided under this Agreement with the accessibility requirements of Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 794d), and its implementing regulations set forth at Title 36, Code of Federal Regulations, Part 1194. Company and College acknowledge that compliance with accessibility requirements involves subjective judgments as to specific methods chosen. Company agrees to promptly respond to any complaint regarding accessibility of its products or services that is brought to its attention. Company further agrees to indemnify and hold harmless College from any claim arising out of Company's failure to demonstrate good faith efforts to achieve and maintain compliance with the aforesaid requirements. Failure to resolve any accessibility issue to the satisfaction of College will be grounds for termination of this Agreement.

C. Supplier warrants that it has and will comply with District's gift ban policy (Board Policy 3821) located here: https://rsccd.edu/Trustees/Documents/Board%20Policies/BPsChapter%203/BP%203821%20Gift%20Ban%20Policy.pdf.

D. Supplier warrants that the signatory of this Agreement is duly and fully authorized to execute this Agreement on behalf of Supplier and to bind the Supplier to each and every term, condition, and covenant of this Agreement.

ARTICLE 14. COMPLIANCE WITH APPLICABLE LAWS

The Parties agree to comply with all federal, state, and local laws, rules, regulations, and ordinance that are now or may in the future become applicable to either party, Supplier's business, equipment and personnel engaged in operations covered by this Agreement or accruing out of the performance of such operations.

ARTICLE 15. MISCELLANEOUS

H. Supplier represents that it is an equal opportunity employer and acknowledges that it shall not

subject any person to unlawful discrimination based on race, color, gender, age, religion, national origin, U.S. military veteran status, marital status, sexual orientation, disability, or political affiliation in programs, activities, services, benefits, or employment in connection with this Agreement. Supplier agrees not to discriminate on any of these bases in its employment or personnel policies, including but not limited to, all activities related to initial employment, upgrading, demotion, transfer, recruitment or recruitment advertising, layoff or termination.

I. The failure of District or Supplier to seek redress for violation of, or to insist upon, the strict performance of any term or condition of this Agreement, shall not be deemed a waiver by that Party of such term or condition, or prevent a subsequent similar act from again constituting a violation of such term or condition.

J. In interpreting this Agreement, it shall be deemed to have been prepared by the Parties jointly, and no ambiguity shall be resolved against District on the premise that it or its attorneys were responsible for drafting this Agreement or any provision hereof. The captions or heading set forth in this Agreement are for convenience only and in no way define, limit, or describe the scope or intent of any Sections/Articles or other provisions of this Agreement. Any reference in this Agreement to a Section/Article, unless specified otherwise, shall be a reference to a Section/Article of this Agreement.

K. Supplier hereby represents, warrants and covenants that (i) at the time of execution of this Agreement, Supplier has no interest and shall not acquire any interest in the future, whether direct or indirect, which would conflict in any manner or degree with the performance of its obligations under this Agreement; (ii) Supplier has no business or financial interests which are in conflict with Supplier's obligations to District under this Agreement; and (iii) Supplier shall not employ in the performance of Work under this Agreement any person or entity having any such interests.

L. Time is of the essence and Supplier shall perform the services required by this Agreement in an expeditious and timely manner so as not to unreasonably delay the purpose of this Agreement.

M. As used in this Agreement, "failure to perform" means failure, for whatever reason, to deliver Goods and/or perform Services as specified in this Agreement. If Supplier fails to performs its obligations under this Agreement, then District, after giving seven days' written notice and opportunity to cure to Supplier, has the right to complete Supplier's obligations itself, to obtain the contracted Goods and/or Services from other suppliers, or a combination thereof, as necessary to complete the work.

N. Except as to any payment due hereunder, Supplier may not assign or subcontract the Agreement without District's written consent. In case such consent is given, the assignee or subcontractor will be subject to all of the terms of the Agreement. Notwithstanding the foregoing, either party may assign this Agreement upon notice to (i) a successor-in-interest as a result of a merger or consolidation or in connection with the sale of all or substantially all of its assets or (ii) an affiliate of such party provided that upon notice, District may terminate this Agreement in accordance with Section 2 of these Terms and Conditions if the District is prohibited from working with the successor business .

G. Unless otherwise agreed upon and in compliance with state, federal, local law, and District policy, during the term of this Agreement and for a period of three years after termination, Supplier shall permit District and its authorized representatives to review all Supplier books, documents, papers, plans, and records, electronic or otherwise ("Supplier Records"), related to this Agreement. Supplier

shall maintain all of Supplier Records in accordance with generally accepted accounting principles so as to document clearly Supplier's performance of the Services. Following final payment and termination of this

Agreement, Supplier shall retain and keep accessible all Records for a minimum of three years, or such longer period as may be required by law, or until the conclusion of any audit, controversy, or litigation arising out of or related to this Agreement, whichever date is later.

H. If the scope of this Agreement requires Supplier to store, retain or otherwise hold District Records (District Records shall be defined as including but not limited to: District's documents, papers, plans, records, electronic or otherwise, actual or in a system) on behalf of the District, District Records shall be held and retained in accordance with and in compliance with state, federal, local law, and District policy, including Board Policy 3310 and Administrative Regulation 3310, Found here https://rsccd.edu/Trustees/Pages/policies-and-regulations.aspx.

ARTICLE 16 – NOTICE

All notices or demands to be given under this Agreement by either Party to the other Party shall be in writing as noted in the Agreement and given either by: (a) personal service, (b) by overnight courier, or (c) by U.S. Mail, mailed either by certified or registered mail, return receipt requested, with postage prepaid to the address listed in this Agreement. Service shall be considered given when received, if personally served, or, if mailed, on the third day after deposit in any U.S. Post Office. The address to which notices or demands may be given by either Party may be changed by written notice given in accordance with the notice provisions of this Article. A Party may change its/his/her designated representative and/or address for the purpose of receiving notices and communications under this Agreement by notifying the other Party of the change in writing and in the manner described in this Article.

ARTICLE 17 – SEVERABILITY

If any term, condition, or provision of this Agreement is held by a court of competent jurisdiction to be invalid, void, or unenforceable, the remaining provisions will nevertheless continue in full force and effect, and shall not be affected, impaired or invalidated in any way.

ARTICLE 18 – FORCE MAJUERE

Neither Party shall be responsible for delays or failure in performance resulting from acts beyond the control of such Parties. Such acts shall include, but not be limited to, Acts of God, labor disputes, civil disruptions, acts of war, epidemics, fire, electrical power outages, earthquakes, or other natural disasters. In claiming a delay or failure to perform under this clause, the delay or failure to perform must be without the fault or negligence of the Party claiming excusable delay or failure to perform and the Party claiming excusable delay must promptly notify the other Party of such delay. Performance under this Agreement shall be considered extended for a period of time equivalent to the time lost due to the force majeure occurrence; however, if such delay continues for a period of more than 30 days, District shall have the option of terminating this Agreement upon written notice to Supplier. Upon such termination for force majeure, the District will pay Supplier for any Goods and/or Services provided in accordance with the Agreement and approved by the District up through the notice of termination. Supplier shall not be entitled to any other costs or damages.

ARTICLE 19 – INELIGIBILITY

If this Agreement is funded in part or whole with federal funds, Supplier certifies to the best of its knowledge and belief that it and its principals are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any federal

department or agency and have not, within a three-year period preceding the execution of this contractual instrument, been convicted of, or had a civil judgment rendered against them, for:

1. Commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State or Local) or private transaction or contract;
2. Violation of Federal or State antitrust statutes;
3. Commission of embezzlement, theft, forgery, bribery, falsification, or destruction of records, making false statements, tax evasion, receiving stolen property, making false claims, or obstruction of justice; or
4. Commission of any other offense indicating a lack of business integrity or business honesty that seriously and directly affects Supplier's present responsibility.

ARTICLE 20 – PARTIES RELATIONSHIP

Supplier will provide the Goods and/or Services as an independent contractor and furnish all equipment, personnel, and supplies sufficient to provide the Services expeditiously and efficiently, during as many hours per shift and shifts per week, and at such locations as District may so require. Supplier will devote only its best-qualified personnel to work under the Agreement. Should District inform Supplier that anyone providing the Services is not working to this standard, Supplier will immediately remove such personnel from providing Services and those individuals will not again be assigned to provide Services without District written permission. At no time will Supplier or Supplier's employees, sub-suppliers, agents, or assigns be considered employees of District for any purpose, including but not limited to workers' compensation provisions. Supplier shall not have the power nor right to bind or obligate District, and Supplier shall not hold itself out as having such authority. Supplier shall be responsible to District for all Services performed by Supplier's employees, agents and subcontractors, including being responsible for ensuring payment of all unemployment, social security, payroll, contributions and other taxes with respect to such employees, agents and subcontractors.

ARTICLE 21 – COUNTERPARTS

This Agreement may be executed in any number of counterparts, each of which shall be deemed an original but all of which together shall constitute one and the same agreement. Any such counterpart containing an electronic, digital, or facsimile signature shall be deemed an original. Execution of this Agreement signifies the Parties' mutual consent to conduct transactions electronically. Pursuant to the California Uniform Electronic Transactions Act ("UETA") (Cal. Civ. Code § 1633.1 et seq.) and California Government Code 16.5, the District reserves the right to conduct business electronically, unless otherwise communicated by the District to stop such electronic transactions, including without limitation to the use of electronic or digital signatures.

ARTICLE 22 – AMENDMENTS

This Agreement may be amended only by written instrument signed by both District and Supplier and approved by the District's Board of Trustees which writing shall state expressly that it is intended by the Parties to amend the terms and conditions of this Agreement.

ARTICLE 22 – GOVERNING LAW AND VENUE

The terms and conditions of this Agreement shall be governed by the laws of the State of California with exclusive jurisdiction and venue in Orange County, California.

ARTICLE 23 - SUPPLIER TERMS

Any additional terms that Supplier includes, whether in whole or in reference, in an order form, an End User Agreement, clickwrap, click through agreement or similar document will be of no force and effect unless District expressly agrees in writing to such terms.

ARTICLE 24 – SURVIVAL CLAUSE

Upon expiration or termination of the Agreement, the following provisions will survive: WARRANTIES; INTELLECTUAL PROPERTY AND DATA RIGHTS; INDEMNITY AND LIABILITY; INSURANCE; CONFIDENTIALITY; and GOVERNING LAW AND VENUE.

---END---

DATA PROTECTION EXHIBIT

ARTICLE 1. INTRODUCTION

A. While providing the Goods and/or Services contemplated by the Agreement, Supplier may gain access to Rancho Santiago Community College District Restricted Data (hereinafter "District Restricted Data") and/or IT Resources (both defined below). In such an event, Rancho Santiago Community College District (hereinafter "District") and Supplier desire to appropriately protect District Restricted Data and IT Resources. The purpose of this Data Protection Exhibit (hereinafter "Exhibit") is to specify Supplier's cybersecurity and risk management responsibilities when Supplier has access to District Restricted Data and/or IT Resources. Supplier shall comply with the terms and conditions set forth in this Exhibit in its collection, receipt, transmission, storage, disposal, use and disclosure of District Restricted Data and be responsible for the unauthorized collection, receipt, transmission, access, storage, disposal, use and disclosure of District Restricted Data under its control or in its possession by all Authorized Employees/Authorized Persons (defined below).

B. Any capitalized terms used here have the meaning ascribed to such terms as set forth in the Agreement or Incorporated Documents to which this Exhibit is attached and made a part.

C. Supplier must provide commercially acceptable cybersecurity and cyber risk management to protect District Restricted Data and/or IT Resources. This must include, but is not limited to the Supplier:

1. Developing and documenting a plan that protects District Restricted Data and IT Resources;
2. Supplier must responsibly execute this plan;
3. Supplier's approach must conform to a recognized cybersecurity framework designed for that purpose;[1]
4. Supplier's information security plan must be supported by a third-party review or certification. Supplier may only use an alternative to a third-party review if approved by the District's Assistant Vice Chancellor, Information Technology Services;
5. Conducting an accurate and thorough assessment of the potential risks to and vulnerabilities of the security of the District Restricted Data and/or IT Resources. Supplier must mitigate anticipated risks effectively. This includes implementing commercially acceptable security policies, procedures, and practices that protect District Restricted Data and/or IT Resources;
6. Updating its plan to effectively address new cybersecurity risks;
7. Complying with pertinent contractual and regulatory responsibilities;
8. [RESERVED];
9. Keeping District informed with timely updates on risks, vulnerabilities, Security Breaches, and Breaches;
10. Keeping District informed of any measures District must perform to ensure the security of District Restricted Data and IT Resources.

D. If, in the course of providing the Goods and/or Services under the Agreement, Supplier engages in

[1] Examples include the latest versions of PCI DSS, NIST CSF, CIS Critical Security Controls, IS0 27000 series, NIST SP 800-53 and NIST SP 800-171.

transactions with District affiliated individuals (including but not limited to: students, staff, faculty, customers, patients, guests, volunteers, visitors, research subjects, etc.), as a benefit and result of the Agreement, Supplier must treat any data about District affiliated individuals that Supplier creates, receives, and/or collects in the course of those transactions with the same level of privacy and security protections and standards as required of District Restricted Data by this Appendix.

E. Supplier agrees to be bound by the obligations set forth in this Appendix. To the extent applicable, Supplier also agrees to impose, by written contract, the same terms and conditions contained in this Appendix on any sub-supplier retained by Supplier to provide or assist in providing the Goods and/or Services to District.

F. To the extent that a requirement of this Appendix conflicts with those of any other District Agreement or Incorporated Document, the most stringent requirement (including but not limited to: least risk to District, shortest time, best practice, etc.) will apply.

ARTICLE 2. DEFINITIONS

A. "Authorized Persons" means (i) Authorized Employees; and (ii) Supplier's contractors, agents, and outsourcers to this Agreement who have a need to know or otherwise access District's Restricted Data to enable Supplier to perform its obligations under this Agreement, and who are bound in writing by confidentiality obligations sufficient to protect District's Restricted Data in accordance with the terms and conditions of this Agreement.

B. "Breach" means: (1) Any disclosure of District Restricted Data to an unauthorized party or in an unlawful manner; (2) Unauthorized or unlawful acquisition of information that compromises the security, confidentiality, or integrity of District Restricted Data and/or IT Resources; or (3) The acquisition, access, use, or disclosure of protected health information (PHI) or medical information in a manner not permitted under the Health Insurance Portability and Accountability Act (HIPAA) or California law.

C. "District Restricted Data" means: Any information or data created, received, and/or collected by District or on its behalf by Supplier, including but not limited to: application logs, metadata, data derived from such data, information provided to Supplier by or at the direction of District, or to which access was provided to Supplier by or at the direction of District, student non-directory data as defined in Board Policy 5040 (located at https://rsccd.edu/Trustees/Documents/Board%20Policies/BPs-Chapter%203/BP%203821%20Gift%20Ban%20Policy.pdf) in the course of Supplier's performance under this Agreement that identifies or can be used to identify an individual (including, without limitation, full names, date of birth, signatures, addresses, telephone numbers, e-mail addresses, information regarding an individual's race, ethnicity, religious or philosophic beliefs, information analyzing an individual's sex life or sexual orientation, and other unique identifiers), including, without limitation, all Highly-Sensitive Personal Information.

D. "Highly-Sensitive Personal Information" means an (i) individual's government-issued identification number (including but not limited to, social security number, taxpayer identification number, passport numbers, driver's license number or state-issued identification number); (ii) financial account number, credit card number, debit card number, credit report information, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account; (iii) precise geolocation data; (iv) personal characteristics, including but not limited to, photographic images (particularly of face or other identifying characteristics); (v) biometric data (including but not limited to, retina scans, voice signatures, or facial geometry, fingerprints or genetic data); (vi) medical information (including but not limited to any information regarding an individual's medical history, mental or physical condition, medical treatment or diagnosis by a health care professional); or (vii) health insurance data (including but not limited to, an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records).

E. "Illicit Code" means: (1) Any code District would not reasonably expect to be present or operating; (2) Hidden software or functionality with adverse or undesired actions or consequences; (3) Code that replicates or transmits District Restricted Data or activates operating systems or other similar services without the express knowledge and approval of District; (4) Code that alters, damages, or erases any District Restricted Data or software without the express knowledge and approval of District; or (5) Code or apparatus that functions in any way as a: key lock, node lock, time-out, "back door," "trap door," "booby trap," "dead drop device," "data scrambling device," or other function, regardless of how it is implemented, which is intended to alter or restrict the use of or access to any District Restricted Data and/or IT Resources.

F. "IT Resource" means: IT infrastructure, cloud services, software, and/or hardware with computing and/or networking capability that is Supplier owned/managed or District- owned, or a personally owned device that stores District Restricted Data, is connected to District systems, is connected to District networks, or is used for District business. IT Resources include, but are not limited to: personal and mobile computing systems and devices, mobile phones, printers, network devices, industrial control systems (including but not limited to: SCADA, PLCs, Operational Technology, etc.), access control systems, digital video monitoring systems, data storage systems, data processing systems, backup systems, electronic and physical media, biometric and access tokens, or Internet of Things (IoT) devices.

G. "Major Change" means: The implementation of a change that could have an effect on the security of an IT Resource or District Restricted Data. The scope includes changes to architectures, processes, tools, metrics, and documentation, as well as changes to IT services and other configuration items. These include changes related to:

1. Technology upgrades or migrations.
2. Responses to Security Breaches.
3. Modifications of scope (data elements, features, location of District Restricted Data, etc.).
4. Regulatory guidance.
5. Law and legal regulations.
6. Responses to risk assessments.
7. [RESERVED]
8. Material updates or shifts in technologies used by Supplier.

H. "Security Breach" means any act or omission that compromises either the security, confidentiality or integrity of District Restricted Data or the physical, technical, administrative or organizational safeguards put in place by Supplier (or any Authorized Persons) that relate to the protection of the security, confidentiality or integrity of District's Restricted Data.

ARTICLE 3. ACCESS TO DISTRICT INFORMATION AND IT RESOURCES

A. Supplier must limit its access to, use of, and disclosure of District Restricted Data and IT Resources to the least invasive degree necessary required to provide the Goods and/or Services.

B. Supplier may not access or use District Restricted Data and IT Resources for any purpose except to provide the Goods and/or Services.

C. For the avoidance of doubt, Supplier may not access, use, or disclose District Restricted Data and IT Resources outside the scope of the Agreement for purposes of, including but not limited to: marketing, advertising, research, sale, or licensing unless expressly approved in writing by District. Any use of District Restricted Data, including when such use is expressly approved in writing by District, must conform at all time with any and all applicable laws and regulations, including and up to any consumer notice requirements.

D. In the event that the Goods and/or Services include the review of a specific Security Breach or a threat to or anomaly in District Restricted Data or IT Resources, Supplier must limit inspection to the least invasive degree necessary required to perform the investigation.

E. Supplier agrees and covenants that it shall: (i) keep and maintain all District Restricted Data in strict confidence, using such degree of care as is required under applicable law and regulations and is appropriate to avoid unauthorized access, use or disclosure; (ii) use and disclose District Restricted Data solely and exclusively for the purposes for which District Restricted Data, or access to it, is provided pursuant to the terms and conditions of this Exhibit, and not use, sell, rent, transfer, distribute, or otherwise disclose or make available District Restricted Data for Supplier's own purposes or for the benefit of anyone other than District, in each case, without District's prior written consent; and (iii) not, directly or indirectly, disclose District Restricted Data to any person other than its Authorized Employees/Authorized Persons without express written consent from District, (iv) be responsible for and remain liable to District for the actions and omissions of Authorized Persons concerning the treatment of District Restricted Data as if they were Supplier's own actions and omissions; (v) subject to Attachment C Master Services Agreement Section 10 Limitation of Liability, be responsible and be liable to District for the actions and omissions of any unauthorized persons that obtain unauthorized access to District Data as a result of Supplier's actions or omissions; and (vi) Supplier will be responsible for having their authorized employees sign documents that require them to comply with Supplier's security policies.

ARTICLE 4. SUPPLIER INFORMATION SECURITY PLAN AND DUTIES

A. Supplier acknowledges that District must comply with information security standards as required by law, regulation, and regulatory guidance, as well as by District's Board Policies, Administrative Regulations and its internal security program, which protect District Restricted Data and IT Resources.

B. Supplier must establish, maintain, comply with, and responsibly execute its information security plan.

C. Supplier warrants its information security plan is in accordance with the requirements of this Article 4 herein. Supplier agrees to make its information security plan available for review upon request by the District. Upon written request, Supplier shall also provide a network diagram outlining Supplier's information technology network infrastructure and all equipment used in relation to fulfilling its obligations under this Agreement, including, without limitation: (i) connectivity to District and all third parties who may access Supplier's network to the extent the network contains District's data; (ii) all network connections including remote access services and wireless connectivity; (iii) all access control devices (for example, firewall, packet filters, intrusion detection and access-list routers); (iv) all back-up or redundant servers; and (v) permitted access through each network connection.

D. Updates to Supplier's information security plan will occur as follows:

1. On an annual basis, Supplier will review its information security plan, update it as needed, and submit it upon written request by District. Such review and update shall be via a process and supporting tools to evaluate and resolve technical vulnerabilities in its systems within reasonable timeframes to address the risk of potential exploitation, or system, or data compromise.
2. In the event of a Major Change, Supplier will review its information security plan, update it as needed, and submit it, upon written request, to District as detailed herein.

E. If Supplier makes any material modifications to its information security plan that will affect the security of District Restricted Data and IT Resources, Supplier must notify District within seventy-two (72)

calendar hours and identify the changes.

F. Supplier's Information Security Plan must:

1. Comply with the Graham-Leach-Bliley Act (hereinafter "GLBA") and follows the guidelines from the National Institute of Standards and Technology's (hereinafter "NIST") Special Public Publication (hereinafter "SP") 800-171, NIST SP 800-53, NIST Cybersecurity Framework, the International Organization for Standardization's standards: ISO/IEC 27001:2005 –Information Security Management Systems – Requirements and ISO-IEC 27002:2005 – Code of Practice for International Security Management, PCI DSS, CIS Critical Security Controls, the Information Technology Library (hereinafter "ITIL") standards, the Control Objectives for Information and related Technology (COBIT) standards or other applicable industry standards for information security and protection of Personal Identifiable Information.
2. Ensure the security (including but not limited to: confidentiality, integrity, and availability) of District Restricted Data and IT Resources through the use and maintenance of all legally required and appropriate administrative, technical, and physical controls that are no less rigorous than accepted industry practices and that all safeguards comply with applicable data protection and privacy laws;
3. Maintain an incident response program to respond to security incidents;
4. Protect against any reasonably anticipated threats or hazards to District Restricted Data and IT Resources and maintain a process and supporting tools to evaluate and resolve technical vulnerabilities in its systems within reasonable timeframes to address the risk of potential exploitation, or system or data compromise;
5. Address the risks associated with Supplier having access to District Restricted Data and IT Resources;
6. Comply with all applicable legal and regulatory requirements for data protection, security, and privacy;
7. Clearly document the cybersecurity responsibilities of each party;
8. Secures business facilities, data centers, paper files, servers, back-up systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability;
9. Implement network, device application, database and platform security;
10. Implement authentication and access controls within media, applications, operating systems and equipment;
11. Encrypt District Restricted Data stored on any mobile media;
12. Encrypt District Restricted Data transmitted over public or wireless networks;
13. Strictly segregate District's Restricted Data from information of vendor or its other customers so that District's Restricted Data is not commingled with any other types of information;
14. Implement appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and providing appropriate privacy and information security training to Supplier's employees;
15. Prevent the sharing of passwords or authentication secrets that provide access to District Restricted Data and/or IT Resources;
16. Prevent the use of passphrases (passwords) or other authentication secrets that are common across customers or multiple unrelated District sites or units;
17. Prevent unauthorized access to District Restricted Data and IT Resources;
18. Prevent unauthorized changes to IT Resources;
19. Prevent the reduction, removal, or turning off of any security control unless replaces with one of equal or higher security capabilities;
20. Prevent the creation of new Supplier accounts to access District Restricted Data and IT Resources without express written approval from District;
21. Prevent the storing, harvesting, or passing through of District credentials (username, password, authentication secret, or other factor); and

22. Prevent the use or copying of District Restricted Data for any purpose not authorized under the Agreement or any associated Statement of Work (SOW).

G. District retains the right to use the Goods and/ or Services to access and, if applicable, retrieve District Restricted Data stored on Supplier's Services infrastructure at any time at District's sole discretion. If District requests the District Restricted Data from Supplier, Supplier will provide District with copies within forty-eight (48) hours, at no cost to District, after receipt of a request from District, and will cooperate with District's reasonable requests in connection with its response.

H. Supplier will return all District Restricted Data to District in a commonly used, non-proprietary, and mutually agreed upon format.

ARTICLE 5. DISTRICT REQUEST AND SUPPLIER COMPLIANCE

A. If Supplier hosts District Restricted Data through Supplier's IT Resources, Supplier must provide District, upon District's written request, with evidence that demonstrates to District's reasonable satisfaction Supplier's adherence to its information security plan (including but not limited to: third-party report, attestation signed by an authorized individual, attestation of compliance by a qualified assessor, or a mutually agreed upon equivalent) upon execution of the Agreement, upon reasonable request (including but not limited to: annually, after Major Changes, and/or as a result of a Security Breach), or as required by any applicable regulatory or governmental authority.

B. Supplier must respond to District's reasonable questions related to cybersecurity controls, Breaches, Security Breaches, or Major Changes, newly published vulnerabilities, and/or risk assessments within ten (10) business days.

C. District may request and perform a security audit using a qualified third party or a mutually agreed upon alternative annually or as a result of a Breach and/or Security Breach.

ARTICLE 6. NOTIFICATION AND DISCLOSURES

A. Within twenty (20) business days, Supplier must notify District regarding changes in Supplier's security posture or IT infrastructure. Such notices must occur:

1. When Major Changes happen.
2. When Supplier becomes aware of a vulnerability that warrants a CVE2 rating of "High" or "Critical," based on the latest CVE version, for which a patch is not yet available or for which Supplier will delay application of an available patch.

B. Supplier must use commercially acceptable efforts to remediate, within twenty (20) business days, any vulnerability rated as CVE High or Critical.[2]

C. In response to Major Changes, Supplier must update its information security plan no later than fifteen (15) days into the next calendar quarter and must provide updated evidence of compliance with the information security plan.

---

[2] Common Vulnerabilities and Exposures (CVE) is a dictionary-type list of standardized names for vulnerabilities and other information related to security exposures maintained by The MITRE Corporation. CVE aims to standardize the names for all publicly known vulnerabilities and security exposures. The goal of CVE is to make it easier to share data across separate vulnerability databases and security tools. The CVE list can be found at: cve.mitre.org

ARTICLE 7. RETURN AND DISPOSAL OF DISTRICT RESTRICTED DATA

A. For the duration of the agreement, the Supplier shall ensure that the District can easily retrieve all their data stored within the system. The data retrieval process must be designed to allow for efficient extraction of large datasets. Specifically, the District shall not be required to download data one record at a time. The Supplier agrees to offer a bulk data export mechanism that enables the District to download all records in a consolidated, machine-readable format such as CSV, JSON, or other commonly used formats. This bulk export process must be user-friendly and accessible to the District without additional fees or undue complexity.

B. [RESERVED]

C. [RESERVED]

ARTICLE 8. NOTICE

Supplier agrees to notify District as soon as feasible, but in no event more than seven (7) days, both orally and in writing, after Supplier receives correspondence or a complaint that relates to a regulation, contractual obligation, Security Breach, or material risk concerning District Restricted Data. For purposes of this Article 8.A, a correspondence or complaint may include, but is not limited to, any communication that originates from law enforcement, regulatory or governmental agencies, government investigators, corporations, or an individual, but excludes normal customer service correspondence or inquiries.

ARTICLE 9. RESPONSE TO BREACHES AND SECURITY BREACHES

A. Reporting of Breach or Security Breach: If Supplier reasonably suspects or confirms a Breach and/or a Security Breach impacting District Restricted Data and/or IT Resources, Supplier must notify District both orally and in writing using the contacts in the Agreement. Supplier must provide such notifications as soon as feasible but in no event more than seven (7) days after the initial suspicion of a Security Breach and/or Breach and (2) as soon as feasible but in no event more than seven (7) days after the initial confirmation of a Security Breach and/or Breach, if Supplier is able to make such a confirmation. Supplier's notification must identify:

1. Contacts for both technical and management coordination;
2. Escalation and identifying information, such as ticket numbers, system identifiers, etc.;
3. The nature of the Breach and/or Security Breach;
4. The District Restricted Data and/or IT Resources affected;
5. What Supplier has done or will do to mitigate any deleterious effect; and
6. What corrective action Supplier has taken or will take to prevent future Security Breaches.

B. Supplier will provide other information as reasonably requested by District.

C. In the event of a suspected Breach and/or Security Breach, Supplier will keep District informed regularly of the progress of its investigation until the incident is resolved.

D. Breach Response or Security Breach Activities: In the event of a Security Breach, Supplier's actions will include but not be limited to:

1. Promptly preserving any potential forensic evidence relating to the Breach and/or Security Breach;
2. Remedying the Breach and/or Security Breach as quickly as circumstances permit;
3. Promptly, but no more than seventy-two (72) calendar hours after the discovery of Breach and/or Security Breach, designating a contact person to whom District will direct inquiries and who will communicate Supplier responses to District inquiries;
4. As rapidly as circumstances permit, assigning/using appropriate resources to remedy, investigate, and document the Breach and/or Security Breach, to restore District service(s) as directed by District, and undertake appropriate response activities;
5. Providing status reports to District regarding Breach and Security Breach response activities, either on a daily basis or a frequency approved by District;
6. Coordinating all media, law enforcement, or other Breach and/or Security Breach notifications with District in advance of such notification(s), unless expressly prohibited by law;
7. Ensuring that knowledgeable Supplier employees are available on short notice, if needed, to participate in District and Supplier initiated meetings and/or conference calls regarding the Breach and/or Security Breach; and
8. Ensuring that knowledgeable Supplier employees and agents participate in after-action analysis, including root cause analysis and preventive action planning.

E. Breaches and Security Breaches – Corrective and Preventive Action: As a result of a Breach and/or Security Breach impacting District Restricted Data and/or IT Resources, and upon District's request, Supplier must prepare a report detailing corrective and preventive actions. The report must include:

1. A mutually agreed upon timeline for the corrective and preventive actions based on the nature of the Breach and/or Security Breach;
2. Identification and description of the root causes; and
3. Precise steps Supplier will take to address the failures in the underlying administrative, technical, and/or physical controls to mitigate damages and future cyber risk.

F. [RESERVED]

G. Grounds for Termination: Any Breach may be grounds for termination of the Agreement by District. Agreement obligations to secure, dispose, and report continue through the resolution of the Breach and/or Security Breach.

ARTICLE 10. ILLICIT CODE WARRANTY[3]

A. Supplier represents and warrants that the Goods and/or Services do not contain Illicit Code.

B. To the extent that any Goods and/or Services have Illicit Code written into them, Supplier will be in breach of this Agreement, and no cure period will apply.

C. Should Supplier learn of the presence of Illicit Code, Supplier will promptly provide District with written notice explaining the scope and associated risk.

[3] This provision does not relate to Supplier's responsibility to protect against malware or viruses that attack the running IT Resource. Such responses are covered under ARTICLE 4 - SUPPLIER'S INFORMATION SECURITY PLAN.

D. Supplier represents and warrants that it will take commercially reasonable steps to promptly remove Illicit Code.

E. Supplier represents and warrants its practices include Secure software engineering and coding practices that are established, documented, and integrated in an official Software Development Life Cycle (SDLC). Supplier shall attend secure development training periodically. Supplier warrants all new code is peer-reviewed and has undergone quality assurance testing prior to being introduced into production. Supplier logically or physically separates environments for development, testing, and production. District Restricted Data is not used in development or testing environments without explicit written consent from District.

ARTICLE 11. BACKGROUND CHECK

A. Before Supplier's Authorized Persons may access District Restricted Data and/or IT Resources, Supplier must conduct a thorough and pertinent background check. Supplier must evaluate the results prior to granting access in order to assure that there is no indication that any Authorized Persons present a risk to District Restricted Data and IT Resources.

B. Supplier must retain each employee's, sub-supplier's, or agent's background check documentation for a period of three (3) years following the termination of the Agreement.

C. Supplier's Authorized Persons must abide strictly by Supplier's obligations under this Agreement. Supplier agrees to maintain a disciplinary process to address any unauthorized access, use, or disclosure of District's Restricted Data by any of Supplier's officers, partners, principals, employees, agents, or contractors.

D. Upon District's written request, Supplier shall promptly identify for District in writing all Authorized Persons as of the date of such request.

ARTICLE 12. DE-IDENTIFIED DATA

Supplier agrees not to attempt to re-identify any and all de-identified student data. De-identified data may only be used by Supplier for purposes permitted under the Family Educational Rights and Privacy Act (hereinafter "FERPA") and its implementing regulations at 34 CFR 99, including:

1. Assisting the District or other governmental agencies in conducting research and/or other studies;
2. Research and development of the Supplier's educational websites, services, and/or other applications and to demonstrate the effectiveness of the Goods and/or Services;
3. For adaptive learning purposes; and
4. For customized student learning.

Supplier agrees to not transfer de-identified student data to any party unless that party agrees in writing not to attempt re-identification, and prior written notice has been given to the District who has provided prior written consent for such transfer. Prior to publishing any document that names the District explicitly or implicitly, Supplier shall obtain the District written approval of the manner in which the de-identified data is presented.

Appendix A

Schedule of Data

Check if access, transmitted or stored by Supplier to deliver the Goods and/or Services

Category of Data	Types of District Restricted Data	Elements	Source
Personal Information	District Restricted Data	☑Full Names ☑Full Address ☑Telephone Number ☑Email Address ☑Signature ☐Religious or Philosophic beliefs	☑Students ☐Employees
Demographics	District Restricted Data	☐Race ☐Ethnicity ☑Date of Birth (excluding students who are a member of an athletic team) ☐Place of Birth ☑Gender ☐Sexual Orientation	☑Students ☐Employees
Government-issued Identification Number	Highly-Sensitive Personal Information	☑Social Security Number ☐Taxpayer Identification Number ☐Passport Number ☐Driver's License or other federal/state issued identification number	☑Students ☐Employees
Financial Data	Highly-Sensitive Personal Information	☐Account Number Credit or Debit Card Number ☐Credit Report Information ☐Personal Identification Password or password that would permit access to an individual's financial account	☐Student ☐Employees

Precise Geolocation Data	Highly Sensitive Personal Information	☐Precise personal location data obtained from cell tower or WiFi triangulation techniques or latitude-longitude coordinates obtained through GPS technology if such data is sufficiently precise to locate an individual or device.	☐Students ☐Employees
Personal Characteristics	Highly-Sensitive Personal Information	☐Photographic images (particularly of face or other identifying characteristics)	☐Students ☐Employees
Biometric data	Highly-Sensitive Personal Information	☐Retina scans, voice signatures or facial geometry ☐Fingerprints ☐Genetic data	☐Students ☐Employees
Medical information	Highly-Sensitive Personal Information	☐ Individual's medical history, mental or physical condition, medical treatment or diagnosis by a health care professional	☐Students ☐Employees
Health Insurance data	Highly-Sensitive Personal Information	☐Individual's health insurance policy number or subscriber identification number ☐Any unique identifier used by a health insurer to identify an individual ☐Any information in an individual's application and claims history, including any appeals records	☐Students ☐Employees

----- END -----

DUALENROLL.COM
MASTER SERVICES AGREEMENT

THIS MASTER SERVICES AGREEMENT, together with all attached Service Addendums and other exhibits, if any (collectively, the "**Agreement**"), is entered into as of the 1st day of June, 2024 (the "**Effective Date**"), by and between **CourseMaven, Inc.**, a Delaware corporation d/b/a **DualEnroll.com**, with its principal offices located at 43498 Butler Place, Leesburg, VA 20176. ("Company") and Rancho Santiago Community College District located at 2323 N Broadway, Santa Ana, CA 92706 ("College").

Company operates DualEnroll.com™, a cloud-based platform that facilitates the college enrollment process for students still in high school ("**DualEnroll**); and College desires to utilize DualEnroll, as set forth in this Agreement.

For good and valuable consideration, the sufficiency of which is hereby acknowledged, the parties to this Agreement agree as follows:

1. Services.

A. "**Service(s)**" means the DualEnroll platform, including any associated applications, components, features and technology, and products and services made available to College in the course of using the Service (**"Service Components"**). Company develops, configures, operates, and maintains the Services, which College will access via a Company-designated web site or IP address.

B. **"Service Addendum(s)"** means the document(s) describing the College configuration requirements, and the applicable fees, together with any additional terms agreed to between the parties regarding the Service(s). Each executed Service Addendum, shall become a part of this Agreement, and constitute an order for such Service(s).

C. "**Service Administrator(s)**" means individuals authorized by College to execute Service Addendums, administer College's use of the Service; and authorize College employees, representatives, and contractors (**"User(s)**") to use the Service on behalf of College, pursuant to the terms of this Agreement.

2. Right to Use Service.

A. Company hereby grants to College a non-exclusive, non-transferable, right to use the Service(s), in object code only, solely (i) for College's own internal business purposes; (ii) during the Term (as defined below) of this Agreement; and (iii) subject to the terms and conditions of this Agreement and applicable Service Addendum. Any and all rights not expressly granted to College are reserved by Company. With respect to the Service, College shall not: (i) license, sublicense, sell, resell, transfer, assign, distribute or otherwise commercially exploit the Service; (ii) modify or make derivative works based upon it; (iii) reverse engineer or otherwise decompile or disassemble; or (iv) make use of it in any way to: (a) build a competitive product or service; (b) build a product using

similar ideas, features, functions or graphics; or (c) copy any of its ideas, features, functions, or graphics. College may use the Service only for legitimate and lawful business purposes and shall not: (i) send spam or otherwise duplicative or unsolicited messages; (ii) send or store infringing, obscene, threatening, libelous, or otherwise unlawful or tortious material, including material harmful to children or in violation of third party privacy rights; (iii) send or store material containing software viruses, worms, Trojan horses or other harmful computer code, files, scripts, agents or programs; (iv) interfere with or disrupt the integrity or performance of the Service or the data contained therein; or (v) attempt to gain unauthorized access to the Service or its related systems or networks. College shall comply with all applicable laws and regulations concerning export, data privacy and protection, and cooperate with Company in connection with compliance thereto. Company retains the right to terminate the Service or this Agreement immediately for any breach by College of this Section.

B. From time to time, routine maintenance and periodic system repairs, upgrades, and reconfigurations may result in temporary impairment or interruption in Service(s). Company does not control access to the Internet or make any warranties with respect to its availability. Company shall attempt to minimize the duration of and schedule any such interruptions outside of normal business hours.

3. College's Responsibilities. College is responsible for all activity by Service Administrators and its Users. College, Service Administrators and its Users shall all abide by the Company's Terms of Service ("**TOS**") available on its website at www.dualenroll.com, which governs the use of Company Services and its network, systems, and facilities ("**Infrastructure**"). Company expressly reserves the right to modify its TOS from time to time. Posting a revised or updated version of the Company TOS on its website shall constitute notice to College. College shall abide by all applicable laws and regulations in connection with College's use of the Service. College shall: (i) notify Company immediately of any known or suspected breach of security or unauthorized use of the Service; and (ii) report to Company immediately and use best efforts to prevent any known or suspected attempts to copy or distribute the Service or Service Components. College will provide to Company in a timely manner (i) notification of any Service-related issues that require assistance; (ii) assistance by a representative of College qualified to address issues related to set up, maintenance, and support of the Services; and (iii) cooperation with any other reasonable Company requests to enable Company to perform its duties hereunder. In the event College does not provide, in a timely manner, the required assistance and/or access, Company may suspend Service(s) and shall not be liable for any deficiency or delay in performance that results from College's failure to cooperate as required, including any remedies under this Agreement.

4. Data Use. In the course of performing its obligations under this Agreement, Company may collect and use data, solely in compliance with the terms of this Agreement, the then current privacy policy of Company, and applicable law. College represents and warrants that unless it has provided written notice to the contrary, College complies with such privacy policy and that, with respect to any content or data it provides to Company it has the right to provide such content or data.

5. Intellectual Property. Each party shall retain all rights, title, and interest, in and to its patents, trademarks, service marks, logos, copyrights, trade secrets, and any other intellectual property ("**Intellectual Property**"). Company expressly retains all rights, title, and interest to DualEnroll, the

Service, Service Components, and all associated Intellectual Property. Any Intellectual Property produced, conceived, or otherwise developed by or for Company hereunder shall be the exclusive property of Company. Each party grants the other a limited, non-exclusive, revocable, nontransferable, non-sub-licenseable, royalty-free license to use certain Intellectual Property of the other party in connection with this Agreement, as designated by and in accordance with the guidelines of such granting party and subject to the terms of this Agreement.

6. Confidentiality. "**Confidential Information**" means all written or oral information, disclosed by one party (the "**Discloser**") to the other (the "**Recipient**"), identified as confidential or that a reasonable person would consider confidential or proprietary based on its nature and the circumstances surroundings its disclosure. The Recipient will keep confidential any Confidential Information disclosed to it by the Discloser; provided such information shall not be considered proprietary once it is in the public domain by no fault of the Recipient. With respect to any Confidential Information, the Recipient shall: (i) maintain confidentiality using the same care that it would use for its own confidential information, but in any event with reasonable care and in accordance with the Family Educational Rights and Privacy Act; (ii) use the confidential information solely in connection with this Agreement; (iii) cease use of such confidential Information immediately upon termination of this Agreement and either return or destroy it upon request of the Discloser; and (iv) not attempt to reverse engineer or create derivate works from or using the Confidential Information. Notwithstanding the foregoing, each Party may disclose Confidential Information to the limited extent required in order to comply with the order of a court or other governmental body, or as otherwise necessary to comply with applicable law, provided that the Party making the disclosure pursuant to the order shall first have given notice to the other Party, if legally permissible, and shall have provided such assistance as may be reasonably requested to limit or prevent such requirement of disclosure.

7. Payment Terms.

A. License Fees: Company shall bill College for the Service for the full License Term, as defined in the applicable Service Addendum, due upon the earlier of 30 days from invoice date or the License Start Date, as defined in such Service Addendum. All amounts are stated and payable in U.S. dollars and exclusive of any taxes. All taxes other than taxes based on Company's net income will be the responsibility of College. All payment obligations are non-cancelable and all amounts paid are non-refundable. Late payments are subject to interest at the rate 1% per month (or the maximum rate permitted by applicable law, whichever is less). Upon notice, Company may suspend or terminate Service if payments are more than thirty (30) days past due. College shall be responsible for all reasonable costs incurred by Company in connection with collecting amounts past due, including without limitation, attorney and collection fees.

B. Intentionally Omitted.

8. Term and Termination.

A. The initial term of this Agreement is stated in the Services Addendum (the "Term") and will automatically renew for successive Terms of the same duration unless either party provides notice of non-renewal at least ninety (90) days prior to expiration of the then-current Term.

B. A party may terminate the Agreement (i) for a breach of the Agreement by the other party not cured within thirty (30) days of receiving notice that it is in breach; (ii) upon notice, if the other party (a) is adjudged insolvent or bankrupt, (b) has instituted against it and not dismissed within thirty (30) days after filing, or institutes any proceeding seeking relief, reorganization or arrangement under any laws relating to insolvency, (c) makes any assignment for the benefit of creditors, (d) appoints a receiver, liquidator or trustee of any of its property or assets, or (e) liquidates, dissolves or winds up its business, or (iii) immediately if any change occurs in any applicable laws or regulations that would, in that party's reasonable opinion, render the party's performance hereunder illegal or otherwise subject to legal challenge.

Upon expiration or termination of this Agreement, all licenses rights granted hereunder shall immediately terminate and each party shall immediately cease using the other party's Intellectual Property and Confidential Information.

9. Representations and Warranties.

A. Each party hereby represents and warrants that: (i) it is a legal entity duly organized, validly existing and in good standing; (ii) it has all requisite corporate power and authority to execute, deliver and perform its obligations hereunder; (iii) it will avoid deceptive, misleading or unethical practices that could adversely affect the performance of the other party's obligations under this Agreement or damage the reputation of the other party; (iv) its performance of its obligations under this Agreement will not knowingly violate any other agreement between such party and any third party, and (vi) its performance related to this Agreement will comply with all applicable law.

B. Except for the express warranties set forth in this agreement and to the maximum extent permitted by applicable law, each party disclaims any and all other representations and warranties, whether express, implied or statutory, including, but not limited to, any warranties of merchantability, fitness for a particular purpose, data accuracy, system integration, title, non-infringement and/or quiet enjoyment. No warranty is made by either party on the basis of trade usage, course of dealing or course of trade.

C. **Software Security and System Performance.** Company shall (i) establish and maintain industry standard technical and organizational measures to help to protect against accidental damage to, or destruction, loss, or alteration of the materials; (ii) establish and maintain industry standard technical and organizational measures to help to protect against unauthorized access to

the Services and materials; and (iii) establish and maintain network and internet security procedures, protocols, security gateways and firewalls with respect to the Services. The Company software and its components are equipped and/or designed with systems intended to prevent industry known system attacks (e.g., hacker and virus attacks) and unauthorized access to confidential information. The Company will maintain and comply with an internal security policy appropriate under industry standards for organizations of similar size and business operations. Company will utilize commercially reasonable best efforts to ensure overall system response times within normal industry standards; College acknowledges that system performance for individual users is impacted by factors including user network configuration and bandwidth and beyond Company's ability to control.

Company will notify the College of any breach of the system College data soon as feasible based on the circumstances but in no event more than 7 days from discovery or detection. Company will maintain professional liability insurance and other coverages (including but not limited to cyber liability insurance) in the event of a breach. The College, may immediately terminate at its sole discretion upon notice of a breach, at no cost to the College.

10. Limitation of Liability. In no event shall either party be liable for any incidental, indirect, special, consequential or punitive damages, regardless of the nature of the claim, including, without limitation, lost profits, costs of delay, any failure of delivery, business interruption, costs of lost or damaged data or documentation or liabilities to third parties arising from any source, even if advised of the possibility of such damages. Except with respect to breaches of confidentiality and indemnification obligations, the cumulative liability of a party for all claims arising from or relating to this Agreement, including, without limitation, any cause of action sounding in contract, tort, or strict liability, shall not exceed the amounts paid or payable under this Agreement during a twelve (12) month period. Any cause of action College may have with respect to the Service(s) shall be barred unless it is commenced or asserted within one (1) year of the earlier of (i) the effective date of expiration or termination of this Agreement; or (ii) the date after the claim or cause of action arises. The failure of Company to enforce any right or provision in this Agreement shall not constitute a waiver of such right or provision unless acknowledged and agreed to by Company in writing.

11. Indemnification. Company at its own expense will indemnify, defend, and hold harmless College and its and their officers, directors, employees and agents, from and against any loss, demand, cause of action, debt or liability ordered by a court or agreed upon in settlement arising out of a third-party claim resulting from patent or copyright infringement or violation of other intellectual property rights or other proprietary rights or licenses, including, without limitation, trademark or trade secret rights related to its Intellectual Property. In the event that the goods or services purchased hereunder are determined to be infringing, or in Company's reasonable determination are likely to be found infringing by a court of competent jurisdiction, then Company shall (at its sole discretion) modify or replace the goods, or re-perform the services, in a non-infringing (but otherwise conforming) manner, or procure any required license. If none of these alternatives are reasonably available, Company will refund to College the amounts actually paid for the infringing goods or services.

12. Indemnification Process. The party seeking indemnification hereunder ("**Indemnified Party**") shall promptly inform the other party ("**Indemnifying Party**") of any suit or proceeding filed against the Indemnified Party for which the Indemnified Party is entitled to indemnification hereunder. The Indemnifying Party may direct the defense and settlement of any such claim, with counsel of its choosing. The Indemnified Party will provide the Indemnifying Party, at the Indemnifying Party's expense, with information and assistance reasonably necessary for the defense and settlement of the claim. The Indemnified Party shall have the right, but not the obligation, at its sole expense to participate in (but not to control) the defense of any such suit or proceeding.

13. Insurance. During the term of this agreement, Company will maintain insurance coverage levels as follows:

a. Commercial general liability and personal injury insurance coverage in the following amounts: $1,000,000 each occurrence, $2,000,000 in the aggregate.
b. Professional liability insurance (errors and omissions) in the amount of $2,000,000 per occurrence and $2,000,000 in the aggregate.
c. Cyber and technology insurance in the amount of $2,000,000 per occurrence and $2,000,000 in the aggregate.
d. Policies will include a waiver of subrogation.

14. Additional Provisions

A. Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the State of California, without regard to conflicts of law.

B. Assignment. Neither party may assign this Agreement without prior written consent of the other party, not to be unreasonably withheld, delayed or conditioned. Notwithstanding the foregoing, either party may assign this Agreement upon notice to (i) a successor-in-interest as a result of a merger or consolidation or in connection with the sale of all or substantially all of its assets or (ii) an affiliate of such party.

C. Survival. The obligations of the Parties which, by their nature, would continue beyond termination or expiration of this Agreement shall survive termination or expiration of this Agreement, including, without limitation, Sections 5-8 and 10-13.

D. Notice. Any notice or other communication which, under this Agreement or otherwise must be given or made by either party, shall be in writing and deemed served when delivered. Notice may be delivered by mail, in person, or by electronic mail to the address provided by each party.

E. General. This Agreement: (i) covers the parties' entire agreement, and supersedes all prior discussions and writings between them, relating to its subject matter; (ii) will be binding upon and inure to the benefit of the parties, their successors and permitted assigns; (iii) creates no agency, partnership or employer-employee relationship between the parties; their relationship is that of

independent contractors; and (iv) has no third party beneficiaries. If any provision in the Agreement is deemed invalid, illegal, or otherwise unenforceable, such provision shall be enforced as nearly as possible in accordance with the parties' intent; the remainder will remain in full force and effect. No failure or delay by a party in enforcing this Agreement shall be construed as a waiver of any of its rights under it. No party shall be deemed in default of this Agreement if the performance of its obligations is delayed or prevented by events beyond its reasonable control.

IN WITNESS WHEREOF, each of the Parties hereto has duly executed and delivered this Agreement as of the Effective Date.

CourseMaven, Inc.	COLLEGE: _____
By: Janet Van Pelt	By: _____
Name: Janet Van Pelt	Name: _____
Title: CEO	Title: _____

RANCHO SANTIAGO
Community College District

DualEnroll

Service Addendum No. 1

1. **License Term, Pricing and Billing**

License Term	**1 years**
License Start Date	**June 1, 2024**
Year One Annual License Fee—Registration only	**$45,044**
One-Time Implementation Fee—	**$30,000**
Invoiceable on Signing	**$75,044**

License fee is based on program size up to 13,000 duplicated registrations across two colleges (Santa Ana and Santiago Canyon) using the same workflow. If duplicated registrations exceed this number in any year, the license fee will adjust for the following year based on the then-current price schedule, but no adjustment will be required for the prior year. Variations in the workflow between colleges may result in additional implementation fees.

2. **Service Components**
   a. Process discovery and design consulting including best practices
   b. Configuration of college-specific workflows
   c. Unlimited user accounts
   d. Access and utilization of the configured DualEnroll.com platform
   e. Training and product orientation recorded and live webinars
   f. Documentation - user guides in PDF format
   g. Support: ticketing with 1 business day response time, phone support for college staff
   h. Reporting

3. **SIS Integration--**
   a. College will provide DualEnroll with access to development and production environments including and make functional stakeholders available for user acceptance testing.

This Service Addendum is approved as of the last date below:

CourseMaven

By: Janet Van Pelt

Name: Janet Van Pelt

Title: CEO

Date: June 5, 2024

COLLEGE: _____

By: _____

Name: _____

Title: _____

Date: _____

ITS Contract Renewal 2025-2026 Forecast

Vendor Name	Contact	Service	FY 23-24 Cost	FY 24-25 Cost	FY 25-26 Forecast Cost	Term	From	To
Ad Astra Information System	A. Howard	Hosting Fee	**$17,624.84**	**$19,387.32**	**$21,326.06**	1	9/20/24	9/19/25
Ad Astra Information System	A. Howard	Astra Schedule Blue (FTE 20,000 or larger, interface maintenance fee)	**$19,812.79**	**$21,794.07**	**$23,973.48**	1	9/20/24	9/19/25
Apogee	J. Gonzalez / D. Clacken	Advising: Cloud migration, design, architecture	**$30,600.00**	**$36,000.00**	**$39,600.00**	1	1/17/24	6/30/24
Aurora Enterprise	D. Clacken	BeyondTrust - Defendpoint licenses and support (formerly Avecto)	**$59,758.00**	**$51,837.00**	**$57,020.70**	1	7/1/24	6/30/25
BlackBeltHelp	J. Gonzalez	BlackBeltHelp Virtual Helpdesk (CEC Only for FY 23-24)	**$118,021.00**			1	7/1/23	6/30/25
AWS (Direct AWS Billing)	D. Clacken	AWS Cloud Computing Resources		**$150,000.00**	**$150,000.00**	1	7/1/24	6/30/25
Calero Software	D. Clacken	VeraSMART Call Accounting System	**$2,989.35**	**$3,049.14**	**$3,354.05**	1	7/1/24	6/30/25
Campus Core LLC	J. Gonzalez	Campus Community Platform: SAC & SCC		**$8,990.00**	**$9,889.00**	1	7/1/24	6/30/25
Carahsoft Technology Corp	A. Howard	Jira Cloud License & App (25)	**$2,641.31**	**$2,875.00**	**$3,162.50**	1	7/1/24	6/30/25

Vendor Name	Contact	Service	FY 23-24 Cost	FY 24-25 Cost	FY 25-26 Forecast Cost	Term	From	To
CCLC Community College League	A. Howard	Turnitin - Plagiarism	**$103,020.04**	**$97,308.33**	**$107,039.16**	1	8/1/24	7/31/25
CDW Government Inc	D. Clacken	Right Fax Servers	**$15,773.16**	**$17,375.71**	**$19,113.28**	1	7/1/24	6/30/25
CDW Government Inc	D. Clacken	Cisco Umbrella Support	**$23,960.00**	**$23,960.00**	**$26,356.00**	1	7/1/24	6/30/25
CDW Government Inc	D. Clacken	Aruba Advisory Ad-Hoc remote Services	**$6,360.00**	**$6,360.00**	**$6,996.00**	1	7/1/24	6/30/25

ITS Contract Renewal 2025-2026 Forecast

Vendor Name	Contact	Service	FY 23-24 Cost	FY 24-25 Cost	FY 25-26 Forecast Cost	Term	From	To
CDW Government Inc	D. Clacken	Aruba Staff and T&M emergency services provision	**$21,200.00**	**$28,675.00**	**$31,542.50**	1	7/1/24	6/30/25
CDW Government Inc	D. Clacken	Premium Support (68) & Veeam Availability Suite Ent Plus (3) & Veeam Backup for O365 subscription (3500 users)	**$69,356.18**	**$132,893.23**	**$146,182.55**	1	7/1/24	6/30/25
CDW Government Inc	D. Clacken	VMWare software license support	**$73,606.00**	**$86,046.48**	**$94,651.13**	1	7/1/24	6/30/25
Coast Electric	D. Clacken	Cleaning of Cameras - District Wide	**$14,400.00**	**$14,400.00**	**$14,400.00**	1	7/1/24	6/30/25
Collegesource Inc	J. Gonzalez	Transfer Evaluation System (TES), CSO & Catalink - SAC & SCC	**$31,442.25**	**$33,328.78**	**$36,661.66**	1	7/1/24	6/30/25
CodeWork Inc	A. Howard	DB Visualizer (14)	**$1,358.00**	**$1,190.00**	**$1,309.00**	1	7/1/24	6/30/25

Vendor Name	Contact	Service	FY 23-24 Cost	FY 24-25 Cost	FY 25-26 Forecast Cost	Term	From	To
Comevo Inc	J. Gonzalez	Online Orientation	**$22,275.00**	**$22,940.00**	**$25,234.00**	1	7/1/24	6/30/25
Computerland of Silicon Valley	SCC Director	Software subscription renewal for Sassafrass K2 Technical Services	**$1,998.00**	**$1,998.00**	**$2,197.80**	1	7/1/24	6/30/25
Computerland of Silicon Valley	D. Clacken	Jetnexus support - Network Load Balancers	**$2,500.00**	**$2,500.00**	**$2,750.00**	1	7/1/24	6/30/25
Computerland of Silicon Valley	D. Clacken	Adobe-Creative Cloud Enterprise	**$105,266.00**	**$115,792.60**	**$127,371.86**	3-3	7/30/22	8/25/25
Computerland of Silicon Valley	J. Gonzalez	Microsoft Campus Agreement Districtwide	**$311,594.88**	**$315,402.12**	**$346,942.33**	5-6	9/15/20	9/30/26
Computer Protection Technology (CPT) / Mitsubishi	D. Clacken	UPS, Batteries, generators for DO, SAC, SCC, DMC PLUS Emergency Hours	**$14,972.00**	**$14,972.00**	**$16,469.20**	1	10/16/23	6/30/24
Convergint Technologies	D. Clacken	Genetec Advantage Software & Hardware, Annual Support and Maintenance		**$11,363.00**	**$12,499.30**	1	9/1/21	9/30/24
Crown Castle (aka Wilcon)	D. Clacken	Fiber Optic Connection/Dark Fiber - Districtwide	**$212,400.00**	**$212,400.00**	**$212,400.00**	3-5	12/1/22	11/30/27
Data Clean Corp	D. Clacken	Data Center - Decontamination - (3) rooms/1x/year / SCC &	**$4,671.00**	**$5,615.00**	**$6,176.50**	1	7/1/24	6/30/25
Diligent Corp	J. Gonzalez	BoardDocs Subscription	**$17,500.00**	**$17,500.00**	**$19,250.00**	1	7/1/24	6/30/25

Vendor Name	Contact	Service	FY 23-24 Cost	FY 24-25 Cost	FY 25-26 Forecast Cost	Term	From	To
Dyntek	D. Clacken	SCCM Professional Services / Staff Aug	**$14,850.00**	**$14,850.00**	**$16,335.00**	1	7/1/24	6/30/25
ECS Imaging Inc	A. Howard	Updates & Maintenance software support - Laserfiche & Quick Fields	**$11,438.00**	**$12,749.77**	**$14,024.75**	1	7/1/24	6/30/25
Educause	J. Gonzalez	Domain name renewal for sac.edu and sccollege.edu	**$154.00**		**$169.40**	3 yrs	7/31/22	7/31/25
Educause	J. Gonzalez	Domain name renewal for rsccd.edu	**$77.00**		**$84.70**	3 yrs	7/31/22	7/31/25
Ellucian Inc.	J. Gonzalez	Software maintenance & licenses: (Colleague for Core, Student, HR & Financial modules), Application Dev Environment, E-commerce, Mobile Application Edition & Application Service Partner	**$576,097.00**	**$578,565.00**	**$636,421.50**	5-5	7/1/20	6/30/25
Ellucian Inc.	J. Gonzalez	Colleague Self-service Financial Aid Maintenance	**$8,337.00**	**$8,754.00**	**$9,629.40**	4-4	7/1/21	6/30/25
Ellucian Inc.	J. Gonzalez	Application Management & Application Hosting Services	**$559,912.68**	**$573,111.00**	**$630,422.10**	4-5	10/1/21	9/30/26
Ellucian Inc.	J. Gonzalez	Professional Services - Phase 2	**$125,000.00**	**$98,120.00**	**$150,000.00**	1-5	6/26/24	6/25/29
Ellucian Inc.	J. Gonzalez	Subscription - Ellucian Payment Center by Touchnet	**$50,879.00**	**$52,405.00**	**$57,645.50**	4-5	10/1/20	6/30/25
Ellucian Inc.	J. Gonzalez	Colleague Self-service Financial Aid Maintenance - CESA Fee	**$2,247.00**	**$2,404.00**	**$2,644.40**	1	7/1/24	6/30/25
Ellucian Inc.	J. Gonzalez	Experience/Insights/Consulting + prorated license		**$124,160.00**		1-2	7/1/24	9/30/26
Ellucian Inc.	J. Gonzalez	Experience/Insights		**$184,000.00**	**$196,880.00**	1-2	7/1/24	9/30/26

Vendor Name	Contact	Service	FY 23-24 Cost	FY 24-25 Cost	FY 25-26 Forecast Cost	Term	From	To
Emergent	SCC Director	Red Hat Enterprise Linux	**$630.00**	**$835.00**	**$918.50**	1	7/1/23	6/30/24
Evisions	A. Howard	Maintenance & Support - Enterprise Fusion Solution	**$3,649.00**	**$3,795.00**	**$4,174.50**	3-3	7/1/22	6/30/25
Evocative	D. Clacken	Delinea Secret Server SaaS (50) Licenses	**$14,788.00**	**$14,172.00**	**$15,589.20**	1	7/1/24	6/30/25
Evocative (Formerly, VPLS Solutions LLC)	D. Clacken	Aruba License & Suppport	**$40,475.88**	**$37,570.99**	**$41,328.09**	1	7/1/24	6/30/25
Evocative (Formerly, VPLS Solutions LLC)	D. Clacken	Multi-Technology Professional Services Assistance: Microsoft SQL, MS Exchange, Aruba Networks, Brocade, Ruckus, Cisco, Palo Alto	**$50,000.00**	**$50,000.00**	**$50,000.00**	1	7/1/24	6/30/25
Evocative	D. Clacken	Exagrid / Serial Numbers EX-AVTA171601039 EX-AVTA171601052 EX-AVTA171601053 EX-AVTA172201135 EX-CT418022000076	**$31,890.55**	**$31,550.74**	**$34,705.81**	1	7/1/24	6/30/25
Evocative	D. Clacken	Exagrid / Serial Numbers EX-CT419101100019			**$0.00**			8/19/25
Evocative	D. Clacken	Exagrid / Serial Numbers EX-CT420113000231			**$0.00**			6/26/26
Faronics	R. Gonzalves	Deep Freeze licenses (1050/ea)	**$3,279.15**	**$3,279.15**	**$3,607.07**	1	7/1/24	6/30/25

Vendor Name	Contact	Service	FY 23-24 Cost	FY 24-25 Cost	FY 25-26 Forecast Cost	Term	From	To
Forsyte	D. Clacken	Guardian365 managed service solution (MSSP) for 24/7/365 systems log monitoring and data/enterprise system protection, Nessuss Vulnerability Reporting Assessment, and Security Program Consulting.	**$3,279.15**	**$113,500.00**	**$124,850.00**	1	7/1/24	6/30/25
Foundation for California Community College (FCCC)	J. Gonzalez	Labster	**$7,740.00**	**$8,514.00**	**$0.00**	1	7/1/24	6/30/25
Foundation for California Community College (FCCC)	J. Gonzalez	Esri (SCC only)	**$2,750.00**	**$0.00**	**$0.00**	1	7/1/24	6/30/25
Golden Star Technology, Inc	D. Clacken	Qognify (formerly) OnSSI Ocularis Support - Camera Licenses (975)	**$47,941.34**	**$45,056.00**	**$49,561.60**	1	7/1/24	6/30/25
Golden Star Technology, Inc	D. Clacken	Annual maintenance for Informacast System & Informacast Moble (Fusion SaaS Subsciption)	**$17,306.00**	**$18,688.00**	**$20,556.80**	1	7/1/24	6/30/25

ITS Contract Renewal 2025-2026 Forecast

Vendor Name	Contact	Service	FY 23-24 Cost	FY 24-25 Cost	FY 25-26 Forecast Cost	Term	From	To
Golden Star Technology, Inc	D. Clacken	Extreme/Brocade Edge Routers @ SAC and SCC Data Center (4x) Serial # CKM2512M066 CKM2513M02S CKM2513M03H CKM2517M036	**$14,452.65**	**$6,407.80**	**$7,048.58**	1	7/1/24	6/30/25
Golden Star Technology, Inc	D. Clacken	Veritas Enterprise Vault (E-Discovery, Storage Mgt & File System Archiving & Search)	**$59,535.00**	**DO NOT PROCESS - Canceling Services**	**$0.00**	1	7/1/23	6/30/24
Golden Star Technology, Inc	Clacken/R. Gonzalves /K. Perna	Samsung / MagicInfo, Digital Signage Perpetual License Support & Maintenance Renewal			**$0.00**			
Golden Star Technology, Inc	D. Clacken	HPe OneView Support and Maintenance Renewal (Quantity 30) HPe_Server Support and Maint Renewal HPe Apollo 4200		**$43,929.74**	**$48,322.71**		7/1/24	6/30/25
Gravic	A. Howard	Remark Office - Scanning Solution	**$550.00**	**$650.00**	**$715.00**	1	7/1/24	6/30/25
Hyland LLC (Formerly Lexmark)	A. Howard	Imagenow licenses	**$49,291.47**	**$52,988.35**	**$58,287.19**	1	7/1/24	6/30/25
Internet2	D. Clacken	InCommon Certificate - Level 4	**$5,000.00**	**$5,000.00**	**$5,000.00**	1	2/1/24	1/31/25
Instructure	J. Gonzalez	Canvas Cloud Subscription 24/7 phone support SAC & SCC	**$26,241.18**	**$28,865.30**	**$31,751.83**	1	7/1/24	6/30/25
JAMF	D. Clacken	Jamf software	**$9,225.00**	**$9,225.00**	**$10,147.50**	1	7/1/24	6/30/25
KLM, Inc	D. Clacken	Data Center - HVAC; SAC, SCC & DMC; PLUS Emergency Hours	**$14,915.00**	**$14,960.00**	**$14,960.00**	1	7/1/24	6/30/25
Mackey LLC	J. Gonzalez	Career Snapshot: SAC & SCC	**$10,000.00**	**$10,000.00**	**$10,000.00**	1	7/1/24	6/30/25

Vendor Name	Contact	Service	FY 23-24 Cost	FY 24-25 Cost	FY 25-26 Forecast Cost	Term	From	To
Nth Generation Computing Inc.	D. Clacken	Cylance Protect Endpoint (N-Side) - 350 clients, 1 year	**$2,488.50**	**$2,593.50**	**$2,852.85**	1	7/1/24	6/30/25
Nth Generation Computing Inc.	D. Clacken	HP Nimble SAN (2x) Arrays DOC S/N: 5UL81102HN (AF-180286) eol = 10/24/2024) SAC S/N: 5UM9320044 (AF-0211515)		**$22,626.00**	**$24,888.60**	1	7/1/24	6/30/25
NeoGov	J. Gonzalez	H/R Management/Recruitment Platform Subscription		**$88,629.45**	**$97,492.40**	1	8/1/24	7/31/25
NextGen	J. Gonzalez	Dynamic Forms	**$7,850.00**	**$15,700.00**	**$17,270.00**	1	7/1/24	6/30/25
NextGen	J. Gonzalez	Scholarship Manager	**$18,895.00**	**$18,895.00**	**$20,784.50**	1	7/1/24	6/30/25
Optiv Security Inc	D. Clacken	Palo Alto Networks	**$177,296.02**	**$188,435.78**	**$207,279.36**	1	7/1/24	6/30/25
O'Reilly Media Inc	J. Gonzalez	Safari Books Online, Technical Book Repository	**$2,569.85**	**$2,619.75**	**$2,881.73**	1	7/1/24	6/30/25
Park Place (Formerly Curvature)	D. Clacken	Annual Software renewal for SMS + SMARTnet - Cisco Gear Support; Proliant Hardware support	**$14,991.84**	**$13,296.48**	**$14,626.13**	1	7/1/24	6/30/25
Pluralsight LLC	A. Howard	Annual license renewal: Academic Professional	**$4,053.00**	**$4,053.00**	**$4,458.30**	1	7/1/24	6/30/25

Vendor Name	Contact	Service	FY 23-24 Cost	FY 24-25 Cost	FY 25-26 Forecast Cost	Term	From	To
Point and Click	J. Gonzalez	Support: Practice Mgt. System - SAC & SCC	**$17,083.00**	**$18,228.00**	**$20,050.80**	1	7/1/24	6/30/25
Recast Software	R. Gonzalves	Right Click Tools	**$12,474.00**	**$13,721.40**	**$15,093.54**	1	11/27/23	11/26/24
SectorPoint Inc	SCC Director	Software support - SWS Dynamic Web Suite for SAC, SCC & DO	**$84,000.00**	**$123,480.00**	**$135,828.00**	1	7/1/24	6/30/25
SectorPoint Inc	SCC Director	Remote service provision (RSP)	**$91,020.00**	**$59,940.00**	**$65,934.00**	1	7/1/24	6/30/25
ServiceNow	J. Gonzalez	Project Management & Ticketing	**$51,975.00**	**$57,172.50**	**$62,889.75**	1-3	4/1/24	3/31/27

Vendor Name	Contact	Service	FY 23-24 Cost	FY 24-25 Cost	FY 25-26 Forecast Cost	Term	From	To
SHI International	D. Clacken	AWS Cloud Computing Resources	**$50,000.00**	**$30,000.00**	**$33,000.00**	1	7/1/24	6/30/25
SHI International	D. Clacken	DuoCircle (AutoSPF)	**$3,600.00**	**$3,697.83**	**$4,067.61**		Starts May 2023	6/30/24
SHI International	D. Clacken	Annual Software support/maint. for Solarwinds	**$16,936.48**	**$18,630.33**	**$20,493.36**	1	7/1/24	6/30/25
SHI International	D. Clacken	Smarsh Inc (SMS Archiving)	**$3,852.21**	**$2,179.91**	**$2,397.90**	1	7/1/24	6/30/25
Sidepath Inc	D. Clacken	Dell VxRail E660F HCS - SCC Data Center	**$10,452.27**		**$11,497.49**	3yr	10/6/22	10/5/25
Sidepath Inc	D. Clacken	Dell Switches S5224F HCS - SCC Data Center	**$1,252.17**		**$1,377.39**	3yr	2/17/23	2/16/26
Sidepath Inc	D. Clacken	PowerEdgeM630 Support Renewal (Service Tag #s: 2D6PV52, 2D6QV52) **EOS = 5/17/2024** PowerEdge M1000E and Force 10 MXL ProSupport renewal (Service Tag #: F2V5Q22)	**$2,453.42**	**$1,500.86**	**$1,650.95**	1	7/1/24	6/30/25

Vendor Name	Contact	Service	FY 23-24 Cost	FY 24-25 Cost	FY 25-26 Forecast Cost	Term	From	To
Sidepath Inc	D. Clacken	PowerEdgeM630 Support Renewal (Service Tag #s: 7JP4C42, 7JP5C42, 7JP6C42, 7JQ4C42) PowerEdgeM620 Support Renewal (Service Tag #F5N6Q22) Force MXL 10_40 Support Renewal (Service Tag #s: 2NZN0Z1, 7MZN0Z1, F2V7Q22, F2VHN22)		**$6,621.74**	**$7,283.91**	1	7/1/24	6/30/25
Sidepath Inc (3rd Party Support due to EOL)	D. Clacken	Ruckus ICX 6610 Essential Remote (Serial #: BXP2502J2BF, BXK2507J0FD, BXK2507J0FL, BXK2507J0FN, BXK2507J0HR, BXK2507J0HZ, BXN2549H1GC, BXN2549H1GD, BXN2549H1GB,BXN2549 H1GE, BXN2549H1G7, BXN2549H1GF, BXK3846K075, BXM2521H00M, BXL2548H0HF & BXL2548H0JB) Ruckus ICX6450 Essential NBD Parts Only Support (Serial #: BZT3227N03A, BZT3227N03R, BZT3227N03T & BZT3227N03W) Ruckus ICX 6450 Essential Remote (Serial #: DVBLHHLOGHG)	**$8,126.38**	**$10,185.12**	**$11,203.63**	1	7/1/24	6/30/25
Sidepath Inc (Direct Ruckus Support)	D. Clacken	Ruckus ICX 7750 Essential Remote Serial # CRH3305L0KJ, CRH3305L00T, CRH3312M0EW, CRH3312M0D3, CRH3305L0KH, CRH3305L0MG,CRH3345 N01A & CRH3344N00D		**$6,830.16**	**$7,513.18**		7/1/24	6/30/25
Sidepath Inc	D. Clacken	Brocade - ESSENTIAL NBD PARTS ONLY SUPPORT RENEWAL, **BR-6510-24 PORT, BR-6510-48 PORT (4)**; (Serial #s: BRW2516K054, BRW2516K055, BRW2548L01C & BRW2548L00C), **BR-6505 (2);** (Serial #s: CCD2519M039 & CCD2519M037)	**$13,743.00**	**$1,943.44**	**$2,137.78**	1	7/1/24	6/30/25

ITS Contract Renewal 2025-2026 Forecast

Vendor Name	Contact	Service	FY 23-24 Cost	FY 24-25 Cost	FY 25-26 Forecast Cost	Term	From	To
Siteimprove Inc	SCC Director	Web Monitoring Service	**$14,999.00**	**$14,999.00**	**$16,498.90**	1	7/1/24	6/30/25
TechnoPro Computer Solutions	A. Howard	ClockWork support plan - SAC & SCC	**$9,456.00**	**$10,164.00**	**$11,180.40**	1	7/1/24	6/30/25
Tech Smith	SCC Director	Camtasia			**$500.00**	3 yrs	9/4/22	9/4/25
Tec Refresh	D. Clacken	ProofPoint Enterprise Archive	**$119,005.74**	**$130,906.31**	**$143,996.95**	1	1/1/24	12/31/24
Touchnet Information Systems	J. Gonzalez	Subscription-Touchnet POS Client & Bill+Payment Mobile	**$19,162.00**	**$19,929.00**	**$21,921.90**	5-5	10/1/20	9/30/25
Touchnet Information Systems	A. Howard	Bluefin Ingenico - Credit Card Readers (4)		**$1,084.00**	**$1,192.40**	13mos	9/1/24	9/30/25
Touchnet Information Systems	A. Howard	Bluefin Ingenico - Credit Card Readers (18)		**$4,500.00**	**$4,950.00**	1	10/1/24	9/30/25
Transource Service Corp	D. Clacken	Exagrid	**$24,149.00**		**$0.00**	3 yrs	3/30/23	3/29/26
Trimdata Corp	A. Howard	FA-Link User Fee - SAC & SCC Bookstore	**$7,000.00**	**$7,700.00**	**$8,470.00**	1	7/1/24	6/30/25
Tyler Technologies, Inc.	D. Clacken	nDiscovery managed solutions for data and enterprise system	**$63,840.00**	**$70,224.00**	**$0.00**	3-3	6/22/21	6/30/24
Tyler Technologies, Inc.	D. Clacken	Cyber Security Partnership Program			**$0.00**	1	7/1/23	6/30/24
Tyler Technologies, Inc.	D. Clacken	Nessuss Vulnerability Assessment			**$0.00**	1	7/1/23	6/30/24
Utelogy Inc	J. Gonzalez	U-Manage Portal - Districtwide	**$6,965.20**	**$6,965.20**	**$7,661.72**	1	7/1/24	6/30/25

Vendor Name	Contact	Service	FY 23-24 Cost	FY 24-25 Cost	FY 25-26 Forecast Cost	Term	From	To
Zoho Corp	D. Clacken	ManageEngine (Subscribtion Based Lic) ADManager Plus Professional Edition 1 Domain (Unrestricted Objects) with 30 help desk Technicians ADAudit Plus Professional Edition for 13 Domain Controllers ADAudit Plus Professional Edition for 2 File Servers ADAudit Plus Professional Edition for 1 Cloud Account for Azure AD tenant account	**$9,602.00**	**$9,602.00**	**$10,562.20**	1	7/1/24	6/30/25
		TOTAL GENERAL FUND	$3,936,321.93	$ 4,591,112.39	$ 4,831,536.81			
		YOY Increase			$ 240,424.42			
		% Increase			4.98%			

DISTANCE EDUCATION TECHNOLOGY

Vendor Name	Contact	Service	FY 23-24 Cost	FY 24-25 Cost	FY 25-26 Forecast Cost	Term	From	To
Foundation for California Community College (FCCC)	A. Howard	Namecoach LTI	**$34,608.00**	**$38,068.80**	**$41,875.68**	1	7/1/24	6/30/25
Foundation for California Community College (FCCC)	J. Gonzalez	NetTutor	**$26,450.00**	**$29,095.00**	**$32,004.50**	1	7/1/24	6/30/25

ITS Contract Renewal 2025-2026 Forecast

Vendor Name	Contact	Service	FY 23-24 Cost	FY 24-25 Cost	FY 25-26 Forecast Cost	Term	From	To
Foundation for California Community College (FCCC)	J. Gonzalez	Pronto	**$68,177.76**	**$74,995.54**	**$82,495.09**	1	7/1/24	6/30/25
Foundation for California Community College (FCCC)	J. Gonzalez	Proctorio	**$39,150.00**	**$43,065.00**	**$47,371.50**	1	7/1/24	6/30/25
Foundation for California Community College (FCCC)	J. Gonzalez	Student Adobe Licenses	**$166,107.45**	**$111,727.65**	**$122,900.42**	1	7/1/24	6/30/25
Golden Star Technology, Inc	D. Clacken	TeamViewer	**$6,739.67**	**$7,020.50**	**$7,722.55**	1	7/1/24	6/30/25
Golden Star Technology, Inc	D. Clacken	Pulse Secure Networks VPN Appliance	**$28,563.84**	**$31,420.22**	**$34,562.25**	1	7/1/24	6/30/25
Ocelot	J. Gonzalez	Ocelot Chatbot	**$280,666.67**	**$135,750.00**	**$149,325.00**	2	4/15/23	4/15/25
Palomar College	D. Clacken	Webinar License - Debra Gerard	**$621.00**	**$621.00**	**$621.00**	1	7/1/24	6/30/25
		TOTAL DE TECHNOLOGY	$651,084.39	$471,763.71	$518,877.98			
		YOY Increase			$47,114.27			
		% Increase			9.08%			

TECHNOLOGY PAID WITH CATEGORICAL FUNDING

Vendor Name	Contact	Service	FY 23-24 Cost	FY 24-25 Cost	FY 25-26 Forecast Cost	Term	From	To

ITS Contract Renewal 2025-2026 Forecast

Vendor Name	Contact	Service	FY 23-24 Cost	FY 24-25 Cost	FY 25-26 Forecast Cost	Term	From	To
Tec Refresh	D. Clacken	ProofPoint Email Security Gateway	**$166,810.00**	**$168,245.00**	**$185,069.50**	1	7/1/24	6/30/25
Invoke Learning	A. Howard	Invoke Clarity Data Platform/Snowflake		**$54,500.00**	**$59,950.00**	1	7/1/24	6/30/25
		TOTAL CATEGORICAL	$166,810.00	$222,745.00	$245,019.50			
		YOY Increase			$22,274.50			
		% Increase			9.09%			
		TOTAL OVERALL	$4,754,216.32	$5,285,621.10	$5,595,434.29			
		YOY Increase			$309,813.19			
		% Increase			5.54%			

Technology Advisory Group

Zoom Meeting (Invitation shared via Outlook)
2:30 p.m. – 4:00 p.m.

Meeting Minutes for September 5, 2024

Voting Members Present: Robert Bustamante, Jesse Gonzalez, Song Le Graham, Scott James, Sergio Rodriguez, Jason Sim, John Steffens, Jason Mondragon Rosas – SAC Student, Valerie Lopez – SCC Student

Voting Members Absent: Pat Weekes

Supporting Members: Dane Clacken, Marvin Gabut, Ron Gonzalves, Adam Howard, William Nguyen, Kimberly Perna

Discussion

Call to Order

- The meeting was called to order by Mr. Gonzalez at 2:32 PM.

1. TAG introductions, membership, responsibilities and purpose.
   - Welcome by Mr. Gonzalez and member introduction. Mr. Jason Sim from SAC is the faculty co-chair for FY 2024-2025.
   - Mr. Gonzalez provided an overview of the membership, responsibilities, and purpose.

2. Annual Report 2023-2024
   - Mr. Gonzalez provided a summary of the report, highlighting how projects are aligned with the districtwide initiatives from the Strategic Technology Plan and in accordance with accreditation standards. The report is regularly presented to TAG and TOW mid and end of year.
   - The report outlines the top ten initiatives by project completion, with "Utilize Hardware Replacement Cycles," "Utilize Software Replacement Cycles," and "Improve Efficiency" as the top three. Projects are prioritized and managed by the operational teams across Infrastructure, Applications, Web, Helpdesk, SAC, and SCC. These areas are overseen by four ITS directors. Mr. Gonzalez used a “house” analogy to provide a visual perspective of each area’s responsibilities.
   - Mr. Sim asked what patterns ITS observed from faculty support tickets and what adjustments could be made. Mr. Gonzalves and Ms. Perna noted that both campuses received faculty requests/issues related to desktops, projectors, printers, and software upgrades for classroom needs.
   - There were 775 completed projects (longer processes) and 19,674 total tickets closed (break/fix issues). On average, 65 projects were completed monthly, and each IT Resource handled approximately 33 tickets per month. The directors reported the following completed projects and outlined their respective areas:
     - Enterprise Applications: Adam Howard – (210 projects completed)
     - Infrastructure and Security: Dane Clacken – (241 projects completed)
     - Helpdesk: Dane Clacken– (48 projects completed)
     - SAC Academic Support: Ron Gonzalves – (116 projects completed)
     - SCC Academic Support: Kimberly Perna – (113 projects completed)

- Web: Kimberly Perna – (47 projects completed): Ms. Perna keyed on the progress of the districtwide web project, Modern Campus CMS implementation.

3. Form task force to develop Strategic Technology Plan (STP) for the following four-year period: Mr. Gonzalez proposed forming a task force to develop the STP for the next four years. This plan will align with the newly completed educational and district strategic plans. The goal is to finalize and present the new technology plan to the Board by Fall 2025. The task force will utilize the fall and spring semesters for development, with implementation planned a year after the educational plans are completed. Mr. Gonzalez suggested including representatives from all constituencies, including non-credit areas, and meeting between TAG meetings. A follow-up email will be sent to the group. Feedback and volunteers for the task force are encouraged.

4. Technology Update:
   - SACTAC: Mr. Steffens provided updated from the May and August meeting.
     - May 2024 meeting:
       - Approval of the Committee Goals and Outcomes.
       - Reviewed TAG action items particularly the 2024-2024 technology initiatives the recommendation against the use of Zoom AI.
       - Distance Ed. reported on the outcome of DE survey. The survey is still in progress.
       - ITS reported the current progress on Windows 11 rollout and classroom upgrades for Fall; and the Pharos printing system outage experienced back in spring that lasted a couple of days.
       - Student Information Support reported on the Ocelot implementation, noting issues with integration and failed tests, and ongoing work with the vendor to resolve them. Addressed the transition of the spider system, which was not functioning yet. Also announced the completion of the Nuventive project and the disbanding of the workgroup, with final configuration for outcomes assessment now completed.
     - August 2024 meeting.
       - Reviewed the membership and accreditation, and the integrated technology plan. Although not expired, discussed updating it to align with SAC's new comprehensive education plan as well as the eventuality of district masterplan alignment.
       - Mr. Sims shared updates on the Net Labs pilot program that is launching at the Cyber Center. This allows students to connect to a virtual desktop and other software.
       - DE Survey shared updates on the survey results highlighting that YouTube is widely used by faculty compared to Pronto. Plan of assessment of their operation. Survey results are posted on the SACTAC team site.
       - ITS reported the current progress on classroom modernization and expected timeline; ongoing Windows 11 rollout and confirmed that faculty, staff and student will have access to Copilot with Windows 11 (currently accessing through Edge browser with district login).
       - Mr. Dane Clacken provided updates on the approval of the requested resources for the hiring of an Information Security Specialist in his department which was approved by the College Council.
       - Mr. Steffens shared updates on the resolution of the Spider issue reported in May, the ongoing Colleague integration, and the successful transition from Cranium Café and other systems included in the process. Also shared the progress of ongoing Starfish implementation where system alerts have been turned on for the Early Childhood and Apprenticeship Program. To better manage user support, the department plans to use ServiceNow, the new IT ticketing system that is currently in the early implementation stage.
       - The college has begun exploring CRM systems which may replace the current Regroup system by the end of the year when its contract expires.

- Library introduction of new dean Dr. Parisa Samaie.
- Ms. Jennifer Hoegger shared the random internet instability at CEC, which is being addressed.
- Student Services shared updates on their involvement in the CRM work group and efforts to improve data management for MIS and other reporting needs.

- SCCTEC: The committee has not met.
- Mr. Rodriguez reported that SCC has been overwhelmed by bots, with 1,000 fraudulent seats reduced to 307 fake students, indicating a drop of nearly 200 FTES from the start of the term to the census date. This issue has somehow resurfaced again, and the challenge is determining where to implement identity verification whether at the CCC Apply level or pre-enrollment. Challenges and workaround to temporarily address some of the issues were shared. Possible solutions need to be discussed. An offline discussion will be scheduled immediately.
- CRM Advise implementation has begun. This is the student success system for SCC. Currently coordinating the SSO and Ellucian Experience student portal in the implementation and related logistics. Just like SAC, SCC is still looking for a CRM tool.

5. Student experience with technology:
   - SCC: Ms. Lopez reported on the computer issue at the B building, classroom 106 and noted a login failure in four different computers. Ms. Perna stated that she will send her team to investigate the issue. She also reported that she was unable to add classes in Self Service but later Unable to add class in Self Service but noted that it was later resolved a week after.
   - SAC Student: No report. Mr. Mondragon Rosas hopes to coordinate with other students for technology-related feedback.

6. Colleague slowness. Mr. Gonzalez reported on the recent Colleague issue that was experienced districtwide. The system's slowness issue was traced to a configuration problem, which we hope to have been resolved. Also announced an upcoming server upgrade scheduled for the 16th, 23rd, and possibly the 30th, all between 10 PM and 6 AM. The team will reach out for testing after each update.

7. Approval of TAG Minutes – May 2, 2024
   - Mr. Gonzalez called for a motion to approve the May 2, 2024, minutes. A motion was made by Mr. J. Nguyen with corrections seconded by Mr. James. Motion passed.

8. Technology Project Listing, August 2024. Mr. Gonzalez moved to table item 8 for the next meeting, seconded by Mr. Rodriguez. Motion passed.

9. District Council Minutes – May 6, 2024, June 3, 2024, July 15, 2024, August 26, 2024. (Informational Attachments)

Informational Handouts

1. ITS Annual Report 2023-2024
2. District Council Minutes – May 6, 2024, June 3, 2024, July 15, 2024, August 26, 2024
3. Top 10 Technology Project Listing – August 2024

Next Meeting Reminder: October 3, 2024, via Zoom

Adjournment

The meeting was adjourned at 4:07 p.m.