RIVERSIDE COUNTY OFFICE OF EDUCATION
3939 Thirteenth Street
Riverside, California 92501

AGREEMENT FOR INFORMATION SYSTEM SUPPORT SERVICES
Business and Student System Support

This Agreement is entered into by and between the **Riverside County Superintendent of Schools**, hereinafter referred to as "SUPERINTENDENT," and the **Perris Union High School District**, hereinafter referred to as "DISTRICT", each being a "Party" and collectively the "Parties".

AGREEMENTS

1. **TERM:** The term of this Agreement shall be from **July 1, 2024 through June 30, 2025.**

2. **SERVICES:** SUPERINTENDENT shall provide the following services:

INFORMATION SYSTEM SUPPORT

A. **Standard Galaxy Support:**
   1. **Service Desk Support**
      a. Process Galaxy Access Form, to add, change and delete screens and users:
         1. Certification of special process to authorize board approved users the approval for Claims Payment and Approve Final Payroll screens.
      b. Incident and Request for Change processing:
         1. Mass updates requests.
         2. Special DB query requests.
         3. Special request reports.
   2. **Reporting and Data Analytics**
      a. Development, scheduling, generation, and distribution of DISTRICT'S Reports, including:
         1. Payrolls (Bi-Weekly, Monthly, Semi-Monthly On-Demand and Annual).
         2. Taxes (Quarterly and Annually).
         3. Financials (Daily, Monthly, Quarterly and Annually).
         4. Fiscal Year End.
         5. Warrants (Payroll and Commercial).
      b. Archival and distribution of electronic versions of reports to be delivered via Email or into report Archive.
      c. Notification of new reports and changes/enhancements to existing reports.
      d. Customization and development of new reports based on DISTRICT's specific requirements.
      e. Maintenance and updating of existing reports as needed to ensure their accuracy and relevance.
      f. Provisioning of Analytic tools to facilitate analysis and reporting activities by DISTRICT's users.
      g. Maintaining and upgrading the data analytic tools to ensure their functionality and compatibility with evolving technologies and data requirements.
      h. Implementing appropriate data security measures, including access controls and user permissions, to safeguard the data analytic tools and the accessed data.
   3. **Special File Transfer Processing**
      a. Process batch claim files.
      b. Payroll direct deposit file processing.
      c. Credit Union file transfer processing.
      d. Custom employee extracts.
      e. Automation of custom data imports and exports to/from Galaxy.

4. **Galaxy maintenance, standard bug fixes, and minor enhancements**
   Unless explicitly stated the Galaxy maintenance window is Sunday, 12 noon to 10 p.m. Service may be interrupted during those hours. Advance notice of downtime is given wherever possible.
5. **Galaxy support website and user group meetings**

B. **Standard RCOE Training Support:**
1. Galaxy, Reporting, and Business Intelligence tools.
2. Specialized training upon request.
   a. Executive style
   b. One-on-one end user training
3. Provide end user documentation for Galaxy, Reporting, and Business Intelligence tools.
   a. System manuals
   b. System enhancement training documents
4. Deployment of new system modules for all supported applications.
5. Office automation training.

C. **Standard Retirement Reporting and Support:**
1. STRS monthly
2. PERS monthly

D. **Optional Services:**
Optional/Additional services and/or products may be purchased at the discretion of DISTRICT on a time and material basis according to this chart to be invoiced separately:

Office automation training with certification (one (1) to nine (9) participants)	$100.00/participant
Office Automation Training without certification (1 to 9 participants)	$65.00/participant
Group (ten (10) or more participants) office automation training with certification	$90.00/participant
Group (10 or more participants) office automation training without certification	$55.00/participant

E. **Galaxy Development/Change Requests**
Change/Enhancement Request(s) should be submitted to the Service Desk. The Galaxy Change Advisory Board is to review all change and project requests and will place in work order for the Development Team if approved. A project request is defined as two (2) or more months of staff time.

3. **DISTRICT'S RESPONSIBLITIES:**

A. **Security and Privacy**
1. **Multi Factor Authentication (MFA):** MFA will be implemented for all individuals accessing Galaxy, Reports, and the Business Intelligence tools.
2. **Secured and Confidential:** Data, reports, or any information that is extracted from SUPERINTENDENT programs are to be kept confidential in a secured environment and not shared with unauthorized individuals.
3. **Access**: Access to SUPERINTENDENT applications must come from devices that have current security patches and antivirus software.

4. **PAYMENT:** The Parties anticipate that there will be monetary obligation on the part of DISTRICT. These are for the following components:

   A. DISTRICT agrees to pay SUPERINTENDENT the amount of **$8.93** multiplied by DISTRICT'S 2023-24 CALPADS enrollment for Galaxy System Support.

   B. DISTRICT agrees to pay SUPERINTENDENT the amount of **$480.00** for Standard Retirement Reporting and Support.

   C. DISTRICT agrees to pay SUPERINTENDENT the amount of **$ .04** per Direct Deposit.

5. **TERMINATION:**
   System Support Services:

   A. Either party may terminate this Agreement, in whole or in part, and without need for cause, by giving 30 day written notice stating the extent and effective date of termination.

   B. Upon any termination pursuant to this Paragraph taking effect, SUPERINTENDENT shall cease all work and services to the extent specified in the termination notice, and DISTRICT shall pay SUPERINTENDENT, in accordance with this Agreement, for all work and services performed prior to termination.

6. **MUTUAL INDEMNIFICATION:**

   A. DISTRICT agrees to indemnify, defend, and hold harmless SUPERINTENDENT, its officers, agents and employees against any claim, liability, loss, injury or damage imposed on SUPERINTENDENT arising out of DISTRICT'S performance on this Agreement, except for liability resulting from the negligent or willful misconduct of SUPERINTENDENT, its officers, agents and employees. If obligated to indemnify, defend, or hold harmless DISTRICT under this Agreement, DISTRICT shall reimburse SUPERINTENDENT for all costs, attorney's fees, expenses and liabilities associated with any resulting legal action. DISTRICT shall seek SUPERINTENDENT approval of any settlement that could adversely affect SUPERINTENDENT, its officers, agents or employees.

   B. SUPERINTENDENT agrees to indemnify, defend, and hold harmless DISTRICT, its officers, agents and employees against any claim, liability, loss, injury or damage imposed on DISTRICT arising out of SUPERINTENDENT'S performance on this Agreement, except for liability resulting from the negligent or willful misconduct of DISTRICT, its officers, agents and employees. If obligated to indemnify, defend, or hold harmless SUPERINTENDENT under this Agreement, SUPERINTENDENT shall reimburse DISTRICT for all costs, attorney's fees, expenses and liabilities associated with any resulting legal action. SUPERINTENDENT shall seek DISTRICT'S approval of any settlement that could adversely affect DISTRICT, its officers, agents or employees.

7. **DATA SECURITY BREACH REPORTING:** California Civil Code 1798.82(a) requires a business, such as a third party provider, or California Civil Code 1798.29(a), requires a state agency, such as SUPERINTENDENT, to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. Any state agency, in accordance with California Civil Code 1798.29(e), or business, in accordance with California Civil Code 1798.82(f), when any single breach occurs that effects 500 or more California residents, is required to electronically submit a sample copy of the security breach notification, excluding any personally identifiable information, to the Attorney General.

8. **PROTECTION OF PUPIL DATA:** California local educational agencies, such as SUPERINTENDENT, and third party providers, are required by federal and state laws to protect certain pupil data, including but not limited to; financial, health, and educational records. SUPERINTENDENT must implement procedures and protective measures to ensure compliance with current federal and state privacy requirements, including but not limited to; California Education Code 49073.1, the Student Online Personal Information Protection Act (SOPIPA), the federal Family Educational Rights and Privacy Act (FERPA), the federal Children's Online Privacy Protection Act (COPPA), and the Children's Internet Protection Act (CIPA).

9. **PRIVACY OF PUPIL RECORDS:** DISTRICT is a local education agency and SUPERINTENDENT is a third party provider subject to all state and federal laws governing education, including but not limited to the California Education Code 49073.1, and the federal Family Educational Rights and Privacy Act (FERPA). The California Education Code 49073.1 states that any technology services agreements entered into, renewed, or amended after January 1, 2015, between a local education agency and a third party provider must include certain terms. These requirements apply to agreements for services that utilize electronic technology, including cloud-based services, for the digital storage, management and retrieval of pupil records, as well as, digital software that authorizes a third party provider of educational software to access, store and use pupil records.

In addition to other penalties, an agreement that fails to comply with the requirements of this section shall be rendered void if, upon notice and a reasonable opportunity to cure, the noncompliant party fails to come into compliance and cure any defect. Written notice of noncompliance may be provided by any Party to this Agreement. All Parties subject to this Agreement, voided under this section, shall return all pupil records in their possession to SUPERINTENDENT.

A. Definitions:

Local Education Agency	Includes school districts, county offices of education, and charter schools.
Third Party	A provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records.
Pupil Records	i. Any information directly related to a pupil that is maintained by the local educational agency. ii. Any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other local educational agency employee.
Pupil-Generated Content	Materials created by a pupil, including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, and account information that enables ongoing ownership of pupil content.
Personally Identifiable Information	Shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of third party provider's software, website, service, or app, including mobile apps, whether gathered by third party provider or provided by local education agency or its users, students, or students' parents/guardians.
Eligible Pupil	A pupil who has reached 18 years of age.

B. In compliance with applicable federal and state laws, **Appendix A, RCOE Data Security Practices and Procedures** describes how SUPERINTENDENT ensures the security and confidentiality of sensitive information and confidential records.

10. **DISPUTES:** Except as otherwise provided in this Agreement, any dispute concerning a question of fact arising under this Agreement, which is not disposed by Agreement, shall be disposed by SUPERINTENDENT which shall furnish the decision in writing. The decision of SUPERINTENDENT shall be final and conclusive until determined by a court of competent jurisdiction to have been fraudulent or capricious, arbitrary, or so grossly erroneous as necessarily to imply bad faith. DISTRICT shall proceed diligently with the performance of the Agreement pending SUPERINTENDENT'S decision.

11. **GOVERNING LAW, JURISDICTION, VENUE, AND SEVERABILITY:** This Agreement shall be governed by the laws of the State of California. Any legal action related to the performance or interpretation of this Agreement shall be filed only in the Superior Court of the State of California located in Riverside, California, and the Parties waive any provision of law providing for a change of venue to another location. Prior to the filing of any legal action, the Parties shall be obligated to attend a mediation session with a third party mediator in an attempt to resolve the dispute. In the event any provision in 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 without being impaired or invalidated in any way. Should action be brought to enforce or interpret the provisions of the Agreement, the prevailing Party shall be entitled to attorney's fees in addition to whatever other relief are granted.

12. **MODIFICATIONS:** This Agreement may only be modified in writing by the mutual consent of the Parties hereto.

13. **INTERPRETATION:** This Agreement shall be interpreted to give effect to its fair meaning and shall be construed as though both Parties prepared it.

14. **ASSIGNMENT:** Unless authorized in writing by both Parties, neither Party shall assign or transfer any rights or obligations covered by this Agreement. Any unauthorized assignment or transfer shall constitute grounds for termination by the other Party.

15. **NO WAIVER OF DEFAULT:** No delay or failure to require performance of any provision of this Agreement shall constitute a waiver of that provision as to that instance or any other instance. Any waiver must be in writing and shall only apply to that instance.

16. **EXECUTION OF COUNTERPARTS:** If this Agreement is executed in counterparts, each counterpart shall be deemed an original and all such counterparts or as many of them as the Parties preserve undestroyed shall together constitute one and the same Agreement.

17. **AUTHORITY**. The Parties warrant and represent that they have the authority to enter into this Agreement in the names, titles, capacities stated herein and on behalf of the entities, persons, or firms named herein and that all legal requirements to enter into this Agreement have been fulfilled.

18. **ENTIRE AGREEMENT:** This Agreement, including any attachments, exhibits or documents incorporated herein, constitutes the entire Agreement between the Parties hereto with respect to the subject matter hereof and no prior or contemporaneous agreements of any kind or nature relating to the same shall be deemed to be merged herein.

IN WITNESS WHEREOF, the Parties have executed this Agreement and shall become effective upon the date it is signed by the last Party to this Agreement.

Riverside County Superintendent of Schools
3939 Thirteenth Street
Riverside, CA 92501

Signed _____
Authorized Signature

_____

Scott S. Price, Ph.D., Chief Business Official
Division of Administration and Business Services
Printed Name and Title

Date _____

Perris Union High School District
155 East Fourth Street
Perris, CA 92570

Signed _____
Authorized Signature

_____

_____
Printed Name and Title

Date _____

APPENDIX A

RCOE Data Security Practices and Procedures

Introduction: RCOE has established an Information Security (InfoSec) Program based on industry best practices and the needs of California K12 systems. The InfoSec program involves several departments, including Operational Support Services, Personnel Services, and Information Technology Services. The departments are primary functional units that will engage with legal counsel and security service/solution providers to develop and execute improvement plans. This plan may be periodically updated to take into account improving practices and technologies and to respond to a changing threat environment. LEA's will be provided with annual updates where there have been material modifications to the practices and procedures stated below.

As of July 20, 2018, the Program has identified the following areas to be part of the continual improvement of the RCOE InfoSec practices.

1. Anti-Virus/Malware Administration and Configuration
   a. Regularly review and examine the policies and procedures related to Anti-virus/Malware controls and the configuration of Anti-virus/Malware software and appliances.
   b. Continual improvement of Anti-virus/Malware software configuration, operation and security.
   c. Provide Anti-virus/Malware training and awareness.
   d. Practice in depth Anti-virus/Malware defense for server and end user computers.

2. Continuity of Operations Plan (COOP) and Disaster Recovery Plan (DRP)
   COOP is the collection of sets of processes and procedures carried out by an organization to ensure that essential business functions continue to operate during and after a disaster. As part of the COOP there is a **DRP**. These are the technical plans developed for specific groups within an organization to allow them to recover a particular business application. RCOE addresses these plans by:

   a. Performing annual Business Impact Analysis with various departments to identify mission critical processes and/or departments and prioritize the recovery processes and/or departments in accordance with their level of criticality.
   b. Secure Executive Oversight and Support for the COOP.
   c. Continual updates of documentation, content, sufficiency, testing and documentation of test results of the plans.

3. Firewall Administration and Configuration

   a. Examine and document the policies and procedures related to the administration of the organizations firewall(s).
   b. Examine and document configuration files and access control lists for the devices and/or applications and operating systems.
   c. Implement least privilege access.
   d. Documentation, content and sufficiency of firewall policies and procedures.
   e. Logical placement of firewalls.
   f. Restricted access to management interfaces.
   g. Continual evaluation of applied rule sets.
   h. Backup, recovery, and storage of configuration files.
   i. Firewall event log review and sufficient storage for retention policy.

4. Network Systems and Database Vulnerability Scanning
   Perform scheduled simulations of attacks on the network and database systems by utilizing industry best of breed tools, which identify the vulnerabilities in the systems and provide recommendations for remediation.

5. Network Monitoring & Intrusion Detection
   a. Regularly review the event logs to identify and correlate unauthorized, unusual, and sensitive access activity, such as:
      1. Attempted unauthorized logical and physical access;
      2. Access trends and deviations from those trends;
      3. Access to sensitive data and resources;
      4. Highly-sensitive privileged access, such as the ability to override security controls;
      5. Access modifications made by security personnel; and
      6. Unsuccessful attempts to logon to a system.
   b. Improve documentation, content and sufficiency of network monitoring and intrusion detection policies and procedures.

6. Patch Management
   a. Regularly review and update systems, configuration, and applications for required systems.
   b. Sufficient testing of systems before and after patching.
   c. Maintain documentation of patch history of required systems.

7. Physical Security
   To prevent unauthorized personnel from gaining direct access to RCOE facilities that house sensitive information, the following areas are under regular review and improvement process:
   a. Documentation, content and sufficiency of physical security policies and procedures.
   b. External: facility perimeter, perimeter lighting, parking areas, parking area lighting, landscaping, exterior building lighting, exterior doors and locks and other entry points.
   c. Internal: doors, windows, ceilings, raised floors, wiring and utility closets, ceilings, attics, basements, crawlspaces, public areas.
   d. Lock and Key control.
   e. Access control including identification systems in use and access points.
   f. Intrusion alarms.
   g. Fire detection, suppression and prevention.
   h. CCTV/digital imaging technologies.
   i. Power system and utility control points.
   j. Documentation, retired network storage, and refuse disposal.
   k. Mail Handling.
   l. Hard copy record storage.
   m. Network Operations Center.

8. Server (Data Center Systems) Administration and Configuration
   Continual improvement of the following areas:
   a. Documentation of server implementations, policies, and procedures.
   b. Hardware, operating system, and application security.
   c. User account policy and rights assignments.
   d. Auditing policies, system changes, user rights, and access to sensitive data.
   e. Event and security log retention and regular review.
   f. Critical file and folder permissions.
   g. Remote access and security.

9. Network Switch and Router Administration and Configuration
   Continual improvement of the following areas:
   a. Develop clear documentation, content and sufficiency of policies and procedures.
   b. Streamline installation, operation and security.
   c. Regular review of configuration.

10. Workstation Administration and Configuration
Continual improvement of the following:
    a. Documentation of workstation policies and procedures.
    b. Hardware security.
    c. Operating System installation, configuration and maintenance (patching).
    d. User account policies and rights assignments.
    e. Event and security log settings and retention.
    f. Critical file and folder permissions.
    g. Remote access and security.

11. Mobile Devices
Regularly examine RCOE's policies and procedures related to administration of the mobile devices assigned to staff and students. The mobile devices include laptops, tablets and smartphones for both RCOE owned devices and personal devices brought onto RCOE's network.

12. Application Security Assessment and Mitigation
The primary objective is to assess how effectively and efficiently RCOE ensures that no single trusted IT system user, administrator, or vendor is able to exploit vulnerabilities in RCOE's IT systems to accomplish and/or conceal an unauthorized diversion of RCOE's assets. Identify where the risk exists and evaluate the controls designed to mitigate this risk. Regularly review, evaluate, and update, if necessary, of the following IT controls:
    a. Database administration practices.
    b. Production control practices.

13. Users Awareness Training
Develop and update timely and relevant training material to raise the level of cybersecurity awareness of users throughout the organization.