Memorandum of Understanding

This Agreement, for Internet Access Services, is entered into this 01 November 2023, by and between the San Pasqual Union School District (herein referred to as "Agency") and the SAN DIEGO COUNTY SUPERINTENDENT OF SCHOOLS (hereinafter referred to as "County") collectively referred to herein as the "Parties."

Recitals

WHEREAS the purpose of this MOU is to provide Internet Access Services and

WHEREAS County and Agency are desirous to enter into an MOU between them, setting out the working arrangements that each of the participants agrees are necessary to support ongoing Internet Service Access via the County

NOW THEREFORE the parties agree as follows:

1) Scope of Work.

The County will:

a. Provide Agency a network port for cross connection of Agency provided circuitry to the County network, up to 100 gigabits per second.
b. Provide Agency with the necessary interconnecting fiber and SFP/SFP+ interfaces between Agency telecommunications provider equipment and County equipment, up to 10 gigabits per second.
c. Conduct network status monitoring and provide outage notifications to designated Agency staff.
d. Allocate IP addresses from the County public IP CIDR block as provided on Attachment A and incorporated herein by reference.
e. Provide to approved Agency staff access to the County ServiceNow platform to report and track problem reports and incidents. County shall be advised in writing of any changes in designated approved staff in advance of the approval by Agency.
f. Collect and analyze network packet captures, NetFlow, SFlow, and/or other packet and meta data from Agency network traffic as deemed necessary by County.
g. Conduct necessary actions to maintain the safety and integrity of the network for all subscribers.
    i. Perform random and/or routine network vulnerability scans of the public IP CIDR block using various methods and tools to identify compromised systems.
    ii. County may perform vulnerability scans of the Agency's internal network and provide results of scans to the Agency for its disposition upon request as provided on Attachment B and incorporated herein by reference.
    iii. Redirect Agency Internet traffic to an on-demand DDoS Mitigation Service (DMS) provided by the California K-12 High Speed Network (K12HSN), if County or the Agency believes there is a denial-of-service attack in progress. The service will

redirect network packets to a third-party scrubbing services and route "clean" traffic back to the County edge.

iv. County may temporarily route Agency data traffic through County firewall(s) for inspection or intrusion detection & prevention analysis upon request.

v. Employ publicly available information to inform an Agency of potential malicious behavior including but not limited to Shodan.

vi. County reserves the right to interrupt the data connection(s) of Agency if County identifies a compromised system and that is negatively impacting the ability of other agencies to fully utilize the service. County will communicate with any affected Agency regarding issues or threats prior to taking significant mitigating action. It is our shared responsibility to defend against cyber-attacks.

h. Respond to urgent network outages reported to County point of contact. County will use its "best efforts" to respond to reported outages outside normal work hours (M-F, 8:00AM to 5:00PM, excluding holidays).

i. County conducts monthly scheduled maintenance that may interrupt service during the maintenance window. County will provide schedule to Agency staff and provide notification of upcoming work.

The Agency will:

a. Provide a point of contact for Agency to receive communications from County pertaining to this service.

b. Maintain a current, signed e-rate letter of Agency with the California K-12 High Speed Network. Agency will also complete K12HSN's annual datalink survey, which will inform bandwidth utilization as well as growth and usage trends needed by the state.

c. Notify County of additional circuitry or bandwidth upgrades no less than 2 months prior to the expected go-live date.

d. Schedule appointments for all routine telecommunications vendor access to County premises two (2) business days in advance.

e. Notify County of all planned service outages (circuit, power, etc.).

f. Provide an IP address on the Agency's network to permit County to conduct connectivity testing (ping) and quality assurance.

g. Provide to County the necessary optical interface equipment for any connection greater than 10 gigabits per second.

h. Mitigate all reported malicious or undesirable network traffic in a timely manner to be agreed upon on a case-by-case basis.

2) Compensation and Reimbursement.

There will be no exchange of funds for the performance of these services. The provision of services is pursuant to the desire of County to ensure Internet access for students within the county of San Diego.

3) Term of Agreement.

This Agreement shall be effective from the period commencing upon November 1st, 2023, and ending June 30, 2024, unless sooner terminated by as provided in the section of the Agreement entitled "Termination."

4) Renewal.

This Agreement shall automatically renew for successive one-year periods, up to no more than 3 renewals, on the same terms and conditions, unless earlier terminated as provided herein.

5) Termination.

This Agreement may be terminated with or without cause by County or Agency. Termination without cause shall be effective only upon 120-day written notice to the other party. During the said 120-day period County shall not revoke use of the network. Upon termination of this agreement, County shall disconnect Agency circuitry from County network equipment. Agency shall return all assigned IP addresses. County shall return any optical interface equipment provided by Agency. This Agreement may be terminated by Agency with cause in the event of a material breach of this Agreement, misrepresentation by County in connection with the formation of this Agreement or the failure to provide benefit to Agency. Termination for cause shall be affected by delivery of written notice of termination to County. Such termination shall be effective upon delivery of said notice.

6) Confidential Relationship.

Agency may from time to time communicate to County certain information to enable County to effectively improve the product. County shall treat all such information as confidential, whether or not so identified, and shall not disclose any part thereof without the prior written consent of the Agency. County shall limit the use and circulation of such information, even within its own organization, to the extent necessary to perform the intendent upgrade or bug fixes. The foregoing obligation of this Paragraph 4, however, shall not apply to any part of the information that (i) has been disclosed in publicly available sources of information; (ii) is, through no fault of County, hereafter disclosed in publicly available sources of information; (iii) is now in the possession of County without any obligation of confidentiality; (iv) is required to be disclosed by operation of law; or (v) has been or is hereafter rightfully disclosed to County by a third party, but only to the extent that the use or disclosure thereof has been or is rightfully authorized by that third party.

County shall not disclose any reports, recommendations, conclusions, or other results without the prior written consent of the Agency. In its performance hereunder, County shall comply with all legal obligations it may now or hereafter have, respecting the information or other property of any other person, firm or corporation.

7) Ownership of Documents.

All final stored information within the database is the property of Agency and shall be delivered to Agency by County upon demand (hereafter, "Deliverables"). County shall own its working papers and any engagement documentation. County also shall own its consultant-related general skills, know-how, expertise, ideas, concepts, methods, techniques, processes, software, materials, or other intellectual property which may have been discovered, created, received, developed, or derived by County either prior to or as a result of providing services under the Agreement, so long as County acquires such information without any unauthorized use or disclosure of confidential information of the Agency.

8) No Assignments.

Neither any part nor all of this Agreement may be assigned or subcontracted. Any assignment or subcontracting in violation of this provision shall be void.

9) Audit.

County agrees to maintain and preserve, until three (3) years after termination of the Agreement with the Agency and to permit the State of California or any of its duly authorized representatives, to have access to and to examine and audit any pertinent records related to this Agreement.

10) Assumption of Risk.

Agency understands that the transactions contemplated by this Agreement are subject to complex risks that may arise without warning and may at times be volatile. Because the losses that may occur can be of unanticipated magnitude, Agency expressly acknowledges that it hereby assumes any and all risks associated with the use of Internet Access Services and accepts such terms and conditions. The County shall have no liability to the Agency or any third party for any liability, problem, loss, or damage resulting from their use or attempted use of the simulation software.

11) Independent Contractor.

It is expressly understood that at all times, while rendering the services described herein, and in complying with any terms and conditions of this Agreement. County is acting as an independent contractor and not as an officer, agent, or employee of the Agency.

12) Indemnification.

Each party shall defend, indemnify, and hold the other party, its officers, employees, and agents harmless from and against any and all liability, loss, expense (including reasonable attorneys' fees), or claims for personal injury (including death) or damages to property arising out of the performance of this Agreement but only in proportion to and to the extent such liability, loss, expense, attorneys' fees, or claims for injury or damages are caused by or result from the negligent or intentional acts or omissions of the indemnifying party, its officers, employees, students, or agents. ...

13) Notices.

Each party will appoint a person to serve as the official contact and coordinate the activities of each party in carrying out this MOU. The appointees of each party are:

County: Scott Blaney
Network Services Manager
858-298-2210
netpeople@sdcoe.net

Agency: Mark Burroughs (name)
Superintendent (title)
760. 747. 0239 (phone)
mark.burroughse sanpasqualunion.net (email)

...

14) Amendment.

No oral or other agreements or understandings shall be effective to modify or alter the written terms of the agreement. This Agreement may be amended or modified only by a written instrument signed by the County and by a duly authorized representative of the Agency.

16) Governing Law/Venue.

In the event of litigation, the Agreement and related matters shall be governed by and construed in accordance with the laws of the State of California. Venue shall be with the appropriate state or federal court located in San Diego County.

17) Compliance with Law.

The parties shall be subject to, and shall comply with, all federal, state, and local laws and regulations applicable to its performance under this Agreement including, but not limited to licensing, employment, purchasing practices, wages, hours, and conditions of employment, including non-discrimination.

18) Entire Agreement.

This Agreement represents the entire Agreement and understandings of the parties hereto and no prior writings, conversations or representations of any nature shall be deemed to vary the provisions hereof. This Agreement may not be amended in any way except by a writing duly executed by both parties hereto.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be duly executed, such parties acting by their representatives being thereunto duly authorized.

By: _____ Date: _____

By: _____ Date: _____
Authorized Representative of Agency

ATTACHMENT A

County IP Primary WAN Address assignment(s) to Agency:

209.66.200.31
209.66.192.43
209.66.194.140

"Attachment B"

Upon request from Agency, SDCOE may agree to work with Agency to perform internal and external vulnerability scans of the Agency network. Information will be gathered through various methods and an executive summary report of findings will be provided to the Agency.

Scope of work

As part of the IT vulnerability assessment, the County will scan the Agency network for vulnerabilities on internal systems and vulnerabilities on external/public-facing systems. Work may include various scanning. activities can include wireless networks, wired networks, virtual infrastructure, firewalls, web applications, and in-house written applications.

Findings and recommendations will be presented in clear and succinct draft and final reports to formulate the "detailed technical report" and basis of the executive summary report to the Agency. The individual report(s) will identify and describe the high-risk areas, include identification and descriptions of mitigating controls for the defined high-risk areas. Each risk area will be assigned a risk rating for the Agency to consider remediation plan.

During the reporting phase, the Agency will have an opportunity to vet the County' findings to ensure that the issues presented are accurate and complete.

After presenting the final report to the Agency's internal stakeholders, an executive summary of the final report will be presented to the Agency's executive management team or Audit Committee as needed.

No Guarantee of Success.

The County shall perform the services in accordance with the standards described in this attachment (Attachment B); provided, however, that the County does not give any assurance or warranty as to any results or success of performing the services.

PROJECT WORK PLAN

The IT security assessment will consist of three phases. These include (1) project initiation, (2) External

and internal vulnerability scan activities, (3) Reporting and Presentation. These phases are further defined below.

Phase 1 – project Initiation and Management Activities

Key County and Agency project team members will meet to review the project structure and detailed work plans, establish project contact and communications procedures, establish workspace, modify project schedules to meet the Agency requirements and determine reporting formats. At this meeting, it is expected that the County will be able to confirm target systems, schedule time for testing, and discuss rules of engagement.

Phase 2 - Vulnerability Assessment Scanning

This phase will encompass External Vulnerability Assessment and Internal Network Vulnerability scan. A brief description of each is listed below as separate tasks. For all activities, the County will work with the Agency to confirm target hosts/IP addresses, and schedule accordingly with the Agency IT staff and management prior to running tools.

Task 2.1 - External Vulnerability Assessment Scanning

The number of target systems and extent of the County' testing will be determined during Phase 1. At a minimum, the County expects that the Agency's network firewalls, external routers, remote access devices (e.g., VPN concentrators), and other Internet-facing systems would be in scope of this task.

Web application testing will be performed in conjunction with external vulnerability. The County team will test the web environment for the inclination toward cross site scripting attacks, buffer overflows, SQL injection, and other web-related vulnerabilities and attack vectors. If any of the Agency's systems is hosted on the cloud, it is the responsibility of the Agency to notify cloud provider and obtain written permission for scanning those systems.

Task 2.2 - Internal Vulnerability Assessment Scanning

Perform vulnerability testing, focusing on the "insider threat" that authorized users present to the Agency. Seek out and assess system-related vulnerabilities that an authorized user or curiosity seeker could potentially exploit to obtain unauthorized access to system resources or cause intentional damage to the Agency's data.

1. Selecting target range of IP addresses or specific systems and running initial host scans to detect available systems and identify system parameters.
2. Confirming that the in-house developed applications (if any) are included in the number of systems to be scanned and subsequently tested.

3. Configuring vulnerability assessment scanners based on systems/devices in scope. Note: Unless otherwise requested, denial of service attacks is disabled.
4. Running our vulnerability assessment scanners (NESSUS) against the selected target systems.
5. Analyzing raw results from vulnerability assessment scans and determining potential weaknesses to exploit.
6. Documenting findings (if any).
7. Presenting findings to the Agency IT staff for remediation.

Phase 3 – Reporting and Presentation

This phase will describe the presentation of findings to Agency. A brief description of each is listed below as separate tasks.

Task 3.1 – Prepare Succinct Draft Reports

Based on the results of Phases 1 and 2, a draft report will be prepared. The report will include the necessary level of detail to allow the document to stand on its own. The tentative and suggested content of the report includes I. Executive Summary; II. Findings and Recommendations; and III. Conclusion.

The Executive Summary section will describe the project and significant findings at a high level suitable for management. The Conclusion will provide an overall opinion statement on the Agency's IT security and risk posture. It also may include supplemental information such as the raw results from our vulnerability assessment scans.

Findings and Recommendations will be a separate report that provides an executive summary and details from our vulnerability scanning activities of the internal and external.

Task 3.2 - Review Reports with the District Project Team, Management. And IT Staff

Provide draft reports for discussion and review with the Agency's project team, management, and IT staff. The review sessions are to provide an opportunity for vetting of findings by the Agency staff, clarifying understandings, and going over recommendations, and opportunities for improvement.

Task 3.3 - Incorporate Feedback and Input from the Agency

The County will collect feedback and input from the Agency during the report review task and incorporate the input as needed. Input those results in a nullification of a finding will be considered and its reasoning will be assessed for applicability in reducing the risk noted in the finding. Based on the input and further clarity obtained, findings may be removed from the final reports.

Task 3.4 - Revise and Deliver Final Reports

Make revisions based upon comments received in the draft report and prepare a final, bound reports with one copy in electronic format. Upon request the County can provide a sanitized

version of the reports for broader disclosure. The draft and final reports will be presented to project participants and others as requested.

Task 3.5 - Present Report Findings and Recommendations to the Agency

The County team will present the reports' findings and recommendations to the Agency's management or other stakeholders (e.g., Board or Audit Committee) as needed. The presentation will focus on high-risk findings and other items mentioned in the Executive Summary and will be kept at a high level. A presentation slide deck will be prepared and distributed to the Agency prior to the meeting.

Point of Contact for internal and external vulnerability scans of an Agency network

County: Francisco Tamayo
Senior Director, Cybersecurity & Digital Privacy
858-290-5566
SecuringInfo@sdcoe.net