Agreement No. 30000-26-R

AGREEMENT BETWEEN THE COUNTY OF SAN MATEO AND PEREGRINE TECHNOLOGIES, INC.

This Agreement is entered into this January 31, 2026, by and between the County of San Mateo, a political subdivision of the state of California, hereinafter called "County," and Peregrine Technologies, Inc. ("Peregrine"), hereinafter also called "Contractor."

* * *

Whereas, pursuant to Section 31000 of the California Government Code, County may contract with independent contractors for the furnishing of such services to or for County or any Department thereof; and

Whereas, it is necessary and desirable that Contractor be retained for the purpose of providing the Services as described in this Agreement and the applicable Exhibits.

Now, therefore, it is agreed by the parties to this Agreement as follows:

1. Exhibits and Attachments

The following exhibits and attachments are attached to this Agreement and incorporated into this Agreement by this reference:

Exhibit A—Services
Exhibit B—Payments and Rates

2. Services to be performed by Contractor

In consideration of the payments set forth in this Agreement and in Exhibit B, Contractor shall perform services for County in accordance with the terms, conditions, and specifications set forth in this Agreement and in Exhibit A.

3. Payments

In consideration of the services provided by Contractor in accordance with all terms, conditions, and specifications set forth in this Agreement and in Exhibit A, County shall make payment to Contractor based on the rates and in the manner specified in Exhibit B.

In no event shall County's total fiscal obligation under this Agreement exceed Three Million Three Hundred Eighty-Six Thousand Two Hundred Eighteen Dollars ($3,386,218).

In the event that the County makes any advance payments, Contractor agrees to refund any amounts in excess of the amount owed by the County at the time of contract termination or expiration. Contractor is not entitled to payment for work not performed as required by this agreement. For clarity, fees for the current subscription period are earned as of the service start date and are non-refundable except as expressly set forth in Exhibit B or an agreed statement of work and shall not be considered advance payments.

4. Term

Subject to compliance with all terms and conditions, the initial term of this Agreement shall be from January 31, 2026 through July 31, 2027. Thereafter, County may, at its option, extend this Agreement for up to two (2) additional one-year terms upon mutual written agreement of the parties, under the pricing and conditions set forth in Exhibit B.

5. Termination

This Agreement may be terminated by the Procurement Director or his/her designee at any time without a requirement of good cause upon thirty (30) days' advance written notice to the other party. Subject to availability of funding, Contractor shall be entitled to receive payment for work/services provided prior to termination of the Agreement.

County may terminate this Agreement or a portion of the services referenced in the Attachments and Exhibits based upon the unavailability of Federal, State, or County funds by providing written notice to Contractor as soon as is reasonably possible after County learns of said unavailability of outside funding.

County may terminate this Agreement for cause. In order to terminate for cause, County must first give Contractor notice of the alleged breach. Contractor shall have five business days after receipt of such notice to respond and a total of ten calendar days after receipt of such notice to cure the alleged breach. If Contractor fails to cure the breach within this period, County may immediately terminate this Agreement without further action. Termination for cause shall not relieve County of its obligation to pay fees accrued and payable through the effective date of termination, consistent with the payment provisions of this Agreement. The option available in this paragraph is separate from the ability to terminate without cause with appropriate notice described above. In the event that County provides notice of an alleged breach pursuant to this section, County may, in extreme circumstances, immediately suspend performance of services and payment under this Agreement pending the resolution of the process described in this paragraph. County has sole discretion to determine what constitutes an extreme circumstance for purposes of this paragraph, and County shall use reasonable judgment in making that determination.

6. Contract Materials

At the end of this Agreement, or in the event of termination, all finished or unfinished documents, data, studies, maps, photographs, reports, and other written materials (collectively referred to as "contract materials") prepared by Contractor under this Agreement shall become the property of County and shall be promptly delivered to County. Upon termination, Contractor may make and retain a copy of such contract materials if permitted by law.

For the avoidance of doubt, Contractor shall not develop, and nothing in this Agreement shall be deemed to require or contemplate the development of, any custom software, custom code, or derivative works for County, and all software provided is standard, pre-existing Contractor technology not prepared under this Agreement.

7. Relationship to Parties

Contractor agrees and understands that the work/services performed under this Agreement are performed as an independent contractor and not as an employee of County and that neither

Contractor nor its employees acquire any of the rights, privileges, powers, or advantages of County employees.

8. Hold Harmless and Limitation of Liability

1 General Hold Harmless

Contractor shall indemnify, defend, and hold harmless County and its officers, agents, employees, and servants from and against any third-party claims, suits, or actions to the extent arising out of Contractor's gross negligence or willful misconduct, and/or Contractor's acts or omissions in the performance of services under this Agreement, and only with respect to the following:

(A) bodily injuries to or death of any person, including Contractor's employees, to the extent caused by Contractor;

(B) damage to tangible property, to the extent caused by the Contractor; or

(C) sanctions, penalties, or claims for damages arising from Contractor's failure to comply, if applicable, with the requirements set forth in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations, solely to the extent such failure is attributable to Contractor's acts or omissions; or

Contractor shall have no obligation to indemnify, defend, or hold harmless County for any claims to the extent arising from the negligence, willful misconduct, or other acts or omissions of County or its officers, agents, employees, or servants.

Contractor's duty to defend any claim under this Agreement is explicitly conditioned on the County's compliance with all requirements herein (including but not limited to prompt notice, etc.) and is explicitly conditioned on a final written finding by the County, following a County investigation into the claim, that such claim arises from Contractor's gross negligence, willful misconduct, and/or Contractor's acts or omissions in the performance of services under this Agreement.

Contractor shall retain control of the defense and settlement of any indemnified claim, provided that no settlement shall impose any obligation or admission on County without County's prior written consent, which shall not to be unreasonably withheld.

2. Intellectual Property Indemnification

Contractor represents and warrants that it owns or has sufficient rights to use the software and services provided by Contractor under this Agreement.

Contractor shall defend, indemnify, and hold harmless County from and against any third-party claim alleging that the unmodified services, as provided by Contractor and used by County in accordance with this Agreement, infringe any enforceable United States patent, copyright, or trademark, and from any final damages awarded by a court of competent jurisdiction and reasonable attorneys' fees directly arising from such claim.

Contractor's obligations under this Section are conditioned upon County:
(a) promptly notifying Contractor in writing of the claim;

(b) reasonably cooperating, at Contractor's expense, in the defense and settlement of the claim; and
(c) permitting Contractor to retain sole control of the defense and settlement of the claim, provided that no settlement shall impose any obligation or admission on County without County's prior written consent, not to be unreasonably withheld.

If the services become, or in Contractor's reasonable opinion are likely to become, the subject of an infringement claim, Contractor shall, at its option and expense, either:
(i) procure the right for County to continue using the services;
(ii) modify the services to make them non-infringing while retaining substantially equivalent functionality; or
(iii) terminate the affected services and refund any prepaid fees for the unused portion of the then-current term.

Contractor shall have no obligation under this Section to the extent any claim arises from:
(a) modifications not made by or at the direction of Contractor;
(b) use of the services in violation of this Agreement;
(c) County-provided data, content, branding, or materials; or
(d) combinations of the services with products or services not provided by Contractor.

Contractor's duty to defend any claim under this Agreement is explicitly conditioned on the County's compliance with all requirements herein (including but not limited to prompt notice, etc) and is explicitly conditioned on a final written finding by the County, following a County investigation into the claim, that such claim arises from Contractor's gross negligence, willful misconduct, and/or Contractor's acts or omissions in the performance of services under this Agreement.

3. <u>Liability Cap</u>

In no event shall Contractor's aggregate liability arising out of or relating to this Agreement under any legal or equitable theory, including breach of contract, tort (including negligence), strict liability, or otherwise, exceed the total amounts paid to Contractor under this agreement in the twelve (12) months immediately preceding the claim.

9. Assignability and Subcontracting

Contractor shall not assign this Agreement or any portion of it to a third party or subcontract with a third party to provide services required by Contractor under this Agreement without the prior written consent of County. Any such assignment or subcontract without County's prior written consent shall give County the right to automatically and immediately terminate this Agreement without penalty or advance notice.

10. Insurance

10.1. General Requirements

Contractor shall not commence work or be required to commence work under this Agreement unless and until all insurance required under this Section has been obtained and is reasonably acceptable to County's Risk Management, such acceptance not to be unreasonably withheld, delayed, or conditioned on requirements inconsistent with this Agreement. Contractor shall furnish County with certificates of insurance evidencing the required coverage, with such certificates evidencing the insurance limits specified in this Agreement. Contractor shall provide certificates of insurance evidencing the required coverage and shall use commercially reasonable efforts to provide County with advance written notice of any material reduction, cancellation, or non-renewal of such coverage.

10.2. Workers' Compensation and Employer's Liability Insurance

Contractor shall have in effect during the entire term of this Agreement workers' compensation and employer's liability insurance providing full statutory coverage. In signing this Agreement, Contractor certifies, as required by Section 1861 of the California Labor Code, that (a) it is aware of the provisions of Section 3700 of the California Labor Code, which require every employer to be insured against liability for workers' compensation or to undertake self-insurance in accordance with the provisions of the Labor Code, and (b) it will comply with such provisions before commencing the performance of work under this Agreement.

10.3. Liability Insurance

Contractor shall maintain, at its own expense and for the duration of this Agreement, commercially reasonable insurance coverage appropriate to the nature of the services performed under this Agreement, including the following minimum coverages:

(a) Commercial General Liability Insurance, including bodily injury and property damage, with a combined single limit of not less than **$1,000,000 per occurrence**;
(b) Automobile Liability Insurance, covering owned, non-owned, and hired vehicles, with a combined single limit of not less than **$1,000,000 per occurrence**; and
(c) Professional Liability (Errors and Omissions) Insurance with limits of not less than **$1,000,000 per claim**.

County and its officers, agents, employees, and servants shall be named as additional insureds on Contractor's Commercial General Liability and Automobile Liability policies, but only with respect to claims arising out of Contractor's acts or omissions in the performance of this Agreement. Such insurance shall be primary and non-contributory with respect to County's insurance to the extent of Contractor's indemnification obligations under this Agreement.

Contractor shall provide certificates of insurance upon request and shall provide reasonable advance written notice of any material reduction or cancellation of required coverage.

In the event Contractor materially fails to maintain the insurance required under this Section, County may, after providing written notice and a reasonable opportunity to cure, suspend performance under this Agreement until such failure is remedied.

10.4. Special Insurance Requirements - Cyber Liability

Cyber Liability	**$5,000,000** per occurrence for Privacy and Network Security, **$1,000,000** per occurrence for Technology Errors and Omissions Such coverage shall be maintained during the term of the Agreement and, to the extent commercially available at reasonable cost, for up to three (3) years thereafter.

If the work involves services or goods related to computers, networks, systems, storage, or access to County data or to any data that may, alone or in combination with other data, become Confidential Information or Personally Identifiable Information, the following insurance is required.

(1) Privacy and Network Security

During the term of the Contract and for three years thereafter, Contractor shall maintain coverage for liability and remediation arising out of unauthorized use of or access to County data or software within Contractor's network or control. Provide coverage for liability claims, computer theft, extortion, network breach, service denial, introduction of malicious code, loss of Confidential Information, or unintentional acts, errors, or omissions by Contractor in the provision of services under this Agreement. The insurance policy shall include coverage for regulatory fines and penalties, and PCI fines and penalties, to the extent such coverage is commercially available and insurable under applicable law, as well as crisis management expenses and business interruption, subject to commercially reasonable sub-limits.

(2) Technology Errors and Omissions

During the term of the Contract and, to the extent commercially available at reasonable cost, for up to three (3) years thereafter, Contractor shall maintain coverage for liabilities arising from errors, omissions, or negligent acts by Contractor in the provision of its standard software-as-a-service offerings and related support services provided under this Agreement, provided that such coverage is obtained as of the Effective Date and maintained thereafter so long as any annual premium increase does not exceed twenty percent (20%) over the premium in effect at contract execution.

11. Compliance With Laws

All services to be performed by Contractor pursuant to this Agreement shall be performed in accordance with all applicable Federal, State, County, and municipal laws, ordinances, regulations, and executive orders, including but not limited to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Federal Regulations promulgated thereunder, as amended (if applicable), the Business Associate requirements set forth in Attachment H (if attached), the Americans with Disabilities Act of 1990, as amended, and Section 504 of the Rehabilitation Act of 1973, which prohibits discrimination on the basis of disability in programs and activities receiving any Federal or County financial assistance, as well as any required

economic or other sanctions imposed by the United States government or under state law in effect during the term of the Agreement. Such services shall also be performed in accordance with all applicable ordinances and regulations, including but not limited to appropriate licensure, certification regulations, provisions pertaining to confidentiality of records, and applicable quality assurance regulations. In the event of a conflict between the terms of this Agreement and any applicable State, Federal, County, or municipal law, regulation, or executive order, the requirements of the applicable law, regulation, or executive order will take precedence over the requirements set forth in this Agreement.

Contractor will timely and accurately complete, sign, and submit all necessary documentation of compliance.

12. Levine Act Compliance

The Contractor certifies and warrants that Contractor has fully complied, and will remain in full compliance, with all applicable requirements of the Levine Act in connection with this Agreement, including making any required disclosures of campaign contributions to County Officers, which includes but may not be limited to elected County Officers. Elected County Officers include members of the San Mateo County Board of Supervisors, as well as the Assessor-County Clerk-Recorder, Controller, Coroner, District Attorney, Sheriff, and Tax Collector-Treasurer. Any campaign contribution required to be disclosed under the Levine Act in connection with this Agreement shall be disclosed on the disclosure form provided by the County of San Mateo Levine Act Disclosure Form, a copy of which is available from the County upon request.

13. Non-Discrimination and Other Requirements

13.1. General Non-discrimination

No person shall be denied any services provided pursuant to this Agreement (except as limited by the scope of services) on the grounds of race, color, national origin, ancestry, age, disability (physical or mental), sex, sexual orientation, gender identity, marital or domestic partner status, religion, political beliefs or affiliation, familial or parental status (including pregnancy), medical condition (cancer-related), military service, or genetic information.

13.2. Equal Employment Opportunity

Contractor shall ensure equal employment opportunity based on objective standards of recruitment, classification, selection, promotion, compensation, performance evaluation, and management relations for all employees under this Agreement. Contractor's equal employment policies shall be made available to County upon request.

13.3. Section 504 of the Rehabilitation Act of 1973

Contractor shall comply with Section 504 of the Rehabilitation Act of 1973, as amended, which provides that no otherwise qualified individual with a disability shall, solely by reason of a disability, be excluded from the participation in, be denied the benefits of, or be subjected to discrimination in the performance of any services this Agreement. This Section applies only to contractors who are providing services to members of the public under this Agreement.

13.4. Compliance with County's Equal Benefits Ordinance

Contractor shall comply with all laws relating to the provision of benefits to its employees and their spouses or domestic partners, including, but not limited to, such laws prohibiting discrimination in the provision of such benefits on the basis that the spouse or domestic partner of the Contractor's employee is of the same or opposite sex as the employee.

13.5. Discrimination Against Individuals with Disabilities

The nondiscrimination requirements of 41 C.F.R. 60-741.5(a) are incorporated into this Agreement as if fully set forth here, and Contractor and any subcontractor shall abide by the requirements of 41 C.F.R. 60–741.5(a). This regulation prohibits discrimination against qualified individuals on the basis of disability and requires affirmative action by covered prime contractors and subcontractors to employ and advance in employment qualified individuals with disabilities.

13.6. History of Discrimination

Contractor certifies that no finding of discrimination has been issued in the past 365 days against Contractor by the Equal Employment Opportunity Commission, the California Department of Fair Employment and Housing, or any other investigative entity. If any finding(s) of discrimination have been issued against Contractor within the past 365 days by the Equal Employment Opportunity Commission, the California Department of Fair Employment and Housing, or other investigative entity, Contractor shall provide County with a written explanation of the outcome(s) or remedy for the discrimination prior to execution of this Agreement. Failure to comply with this Section shall constitute a material breach of this Agreement and subjects the Agreement to immediate termination at the sole option of the County.

13.7. Reporting; Violation of Non-discrimination Provisions

Contractor shall report to the County Executive Officer the filing in any court or with any administrative agency of any complaint or allegation of discrimination on any of the bases prohibited by this Section of the Agreement or the Section titled "Compliance with Laws". Such duty shall include reporting of the filing of any and all charges with the Equal Employment Opportunity Commission, the California Department of Fair Employment and Housing, or any other entity charged with the investigation or adjudication of allegations covered by this subsection within 30 days of such filing, provided that within such 30 days such entity has not notified Contractor that such charges are dismissed or otherwise unfounded. Such notification shall include a general description of the circumstances involved and a general description of the kind of discrimination alleged (for example, gender-, sexual orientation-, religion-, or race-based discrimination).

Violation of the non-discrimination provisions of this Agreement shall be considered a breach of this Agreement and subject the Contractor to penalties, to be determined by the County Executive Officer, including but not limited to the following:

i. termination of this Agreement;

ii. disqualification of the Contractor from being considered for or being awarded a County contract for a period of up to 3 years;

iii. liquidated damages of $2,500 per violation; and/or

iv. imposition of other appropriate contractual and civil remedies and sanctions, as determined by the County Executive Officer.

To effectuate the provisions of this Section, the County Executive Officer shall have the authority to offset all or any portion of the amount described in this Section against amounts due to Contractor under this Agreement or any other agreement between Contractor and County.

14. Compliance with County Employee Jury Service Ordinance

Contractor shall comply with Chapter 2.85 of the County's Ordinance Code, which states that Contractor shall have and adhere to a written policy providing that its employees, to the extent they are full-time employees and live in San Mateo County, shall receive from the Contractor, on an annual basis, no fewer than five days of regular pay for jury service in San Mateo County, with jury pay being provided only for each day of actual jury service. The policy may provide that such employees deposit any fees received for such jury service with Contractor or that the Contractor may deduct from an employee's regular pay the fees received for jury service in San Mateo County. By signing this Agreement, Contractor certifies that it has and adheres to a policy consistent with Chapter 2.85. For purposes of this Section, if Contractor has no employees in San Mateo County, it is sufficient for Contractor to provide the following written statement to County: "For purposes of San Mateo County's jury service ordinance, Contractor certifies that it has no full-time employees who live in San Mateo County. To the extent that it hires any such employees during the term of its Agreement with San Mateo County, Contractor shall adopt a policy that complies with Chapter 2.85 of the County's Ordinance Code." The requirements of Chapter 2.85 do not apply unless this Agreement's total value listed in the Section titled "Payments", exceeds two-hundred thousand dollars ($200,000); Contractor acknowledges that Chapter 2.85's requirements will apply if this Agreement is amended such that its total value exceeds that threshold amount.

15. Retention of Records; Right to Monitor and Audit

(a) Contractor shall maintain all required records relating to services provided under this Agreement for three (3) years after County makes final payment and all other pending matters are closed, and Contractor shall be subject to the examination and/or audit by County, a Federal grantor agency, and the State of California.

(b) Contractor shall comply with all program and fiscal reporting requirements set forth by applicable Federal, State, and local agencies and as required by County.

(c) Contractor agrees upon reasonable notice to provide to County, to any Federal or State department having monitoring or review authority, to County's authorized representative, and/or to any of their respective audit agencies access to and the right to examine all records and documents necessary to determine compliance with relevant Federal, State, and local statutes, rules, and regulations, to determine compliance with this Agreement, and to evaluate the quality, appropriateness, and timeliness of services performed.

16. Merger Clause; Amendments

This Agreement, including the Exhibits and Attachments attached to this Agreement and incorporated by reference, constitutes the sole Agreement of the parties to this Agreement and correctly states the rights, duties, and obligations of each party as of this document's date. In

the event that any term, condition, provision, requirement, or specification set forth in the body of this Agreement conflicts with or is inconsistent with any term, condition, provision, requirement, or specification in any Exhibit and/or Attachment to this Agreement, the provisions of the body of the Agreement shall prevail. Any prior agreement, promises, negotiations, or representations between the parties not expressly stated in this document are not binding. All subsequent modifications or amendments shall be in writing and signed by the parties.

17. Controlling Law; Venue

The validity of this Agreement and of its terms, the rights and duties of the parties under this Agreement, the interpretation of this Agreement, the performance of this Agreement, and any other dispute of any nature arising out of this Agreement shall be governed by the laws of the State of California without regard to its choice of law or conflict of law rules. Any dispute arising out of this Agreement shall be venued either in the San Mateo County Superior Court or in the United States District Court for the Northern District of California.

18. Notices

Any notice, request, demand, or other communication required or permitted under this Agreement shall be deemed to be properly given when both: (1) transmitted via email to the email address listed below; and (2) sent to the physical address listed below by either being deposited in the United States mail, postage prepaid, or deposited for overnight delivery, charges prepaid, with an established overnight courier that provides a tracking number showing confirmation of receipt.

In the case of County, to:

Name/Title: Jas Sandhar/Procurement Manager
Address: 455 County Center, Redwood City, CA, 94063
Telephone: (650) 400-5510
Email: jsandhar@smcgov.org

In the case of Contractor, to:

Name/Title: Nick Noone, CEO, Peregrine Technologies,
Address: PO Box 7775 PMB 69596, San Francisco, CA, 94120-7775
Telephone: (415) 287-2749
Email: nick@peregrine.io, with a copy to ben@peregrine.io

19. Electronic Signature

Both County and Contractor wish to permit this Agreement and future documents relating to this Agreement to be digitally signed in accordance with California law and County's Electronic Signature Administrative Memo. Any party to this Agreement may revoke such agreement to permit electronic signatures at any time in relation to all future documents by providing notice pursuant to this Agreement.

20. Payment of Permits/Licenses

Contractor bears responsibility to obtain any license, permit, or approval required from any agency for work/services to be performed under this Agreement at Contractor's own expense

prior to commencement of said work/services. Failure to do so will result in forfeit of any right to compensation under this Agreement.

21. Cloud Computing Policy 2020

21.1. Overview

Cloud computing is defined as on-demand delivery of information technology (IT) resources through the Internet. Such services use a pool of shared resources to achieve economies of scale, provide greater flexibility, and support communication, collaboration, scheduling, sharing, and storage. In most cases, these services are provided on a contractual basis by a third-party vendor and essentially becomes an extension of the County's network. Security concerns in cloud computing include, but are not limited to:

- Loss of control over the maintenance and protection of the data
- Potential loss of privacy due to aggregation of data from other cloud consumers
- Reliance on vendor's services for the security of County data

21.2. Policy Purpose

The purpose of the Cloud Computing Policy is to safeguard the County's data and to mitigate any risks associated with utilizing cloud solutions. This policy outlines best practices to ensure that data will be properly stored and shared when using cloud computing services.

21.3. Scope

The scope of this policy includes all users of the County of San Mateo's network who uses cloud computing services, including vendors, contractors, volunteers, temporary staff, consultants, collectively known as Workforce Members, and any other party who provides services or works on the computer and/or network systems.

21.4. Policy

All cloud computing services shall undergo a security assessment, performed at the time of contract, including but not limited to: security controls, identity and authentication management, password management, auditing, and encryption capabilities. As part of the review process, all cloud services that are currently listed in the Federal Risk Authorization Management Program (FedRAMP) will undergo an abbreviated security review process. Cloud services that are not "FedRAMPed" will undergo a more in-depth security review process. Any cloud service's security level and trustworthiness must match the sensitivity of the data stored on that service. If there are circumstances that fall outside the ability to comply with and/or conform to County policies, an exception waiver may be required.

All cloud computing services must be reviewed and approved by the Chief Information Officer (CIO) or designee before purchase or deployment, including renewals. The CIO or designee has the right to deny the request and shall provide the reason(s) for doing so as well as alternatives so that a mutually agreeable solution can be developed.

The use of cloud computing services shall comply with all current laws and regulations as well as all County policies. All software stored in the cloud must comply with licensing agreements

and copyright laws. Additionally, all internet domains (URLs) associated with County business shall be managed and registered through ISD.

21.5. Software as a Service

Software as a Service (SaaS) solutions must utilize latest version of Security Assertion Markup Language (SAML) authentication (WS-Federation and Okta's Secure Web Authentication (SWA) may be used in lieu of SAML) and integrate with the County's identity provider (currently Okta). Multi-factor authentication is required when the application is accessed from outside of the County's network. If solutions do not utilize SAML authentication or multi-factor authentication, a request for exception, signed by the Department Head, must be submitted to the CIO or designee, for approval. Note: The security assessment may result in a request for exception based on the results of the review and is not limited to the above-mention authentication processes.

The cloud environment shall also include a County-approved warning banner upon logon, if capable.

All software must be configured to have a lock-out session after thirty (30) minutes of idle time. Full auditing, in coordination with ISD, must be enabled to allow for successful and unsuccessful account logon events, account management events, and system events. Audit logs, if performed by another organization, shall be shared with the County upon request or as stated in the underlying agreement. All audit logs must be stored for a minimum of one year.

Contingency plans for disaster recovery must be provided by the vendor in all SaaS solutions including a strategy to restore the data within a specified time frame.

Both vendor and County roles and responsibilities shall be clearly stated including enforcement mechanisms to meet the required service levels. All parties must also comply with Administrative Memorandum B-1.

The terms and conditions of termination shall be clearly defined along with the disposal and/or transfer of data.

21.6. Confidential Data

Cloud systems are subject to the same internal standards as those located on-premises. Confidential data may only be stored and managed through a secure vendor that has been approved by ISD as appropriate for confidential data.

All vendors shall comply with all County specified standards and requirements in addition to federal and state mandated standards, such as HIPAA. Compliance shall be detailed within the business case for each application. Vendors must provide information regarding the controls they employ to maintain security on all HIPAA and PII data. The following list includes security concerns that will be evaluated in the security review process. Note that an exception waiver may be required in the event that the listed County requirements are not met.

- How and where vendor encrypts data, both at rest and in motion
- How vendor employees who will have physical access to the network and infrastructure that hosts the application, are vetted

- What third-party audits will be/have been performed to validate vendor controls • What security features are and are not included as part of their SLA
- What constitutes a security event and what their notification policies and procedures are after a security event occurs
- If the backups of the County's data are moved offsite, how are they encrypted • How will data be securely deleted or destroyed as requested
- The vendor's ability to provide patches and update products, including the patch schedules and timeline for end-of-device support
- Assurance that the sharing of the County provided account password will be strictly prohibited

Client data from the cloud may not be transmitted to a personal computing device (such as a flash/thumb drive).

21.7. Other County Policies

The County has other policies that address specific areas of information security including policies on IT security, Internet use, email, mobile technology use, vendor/contractor access, and portable computing. These policies are also applicable and extend to cloud services including the use and storage of information. Departments may have internal policies that also address these issues. These policies are cumulative and in the event of conflict, the policies providing the County with the greatest level of security shall apply.

21.8. Responsibility

Departments shall be responsible for providing security awareness and training to all users of devices or electronic media containing Personal Health Information (PHI) or PII as it relates to the HIPAA requirements for all data under their control. ISD will be responsible for providing Countywide security awareness and training

21.9. Policy Enforcement

The CIO or designee is the policy administrator for information technology resources and will ensure that this process is followed. Additionally, Division Directors, managers, and Department Heads are responsible for compliance with County policies within their respective administrative areas.

Any violations of this policy shall be reported to the CIO or designee. Violations will be investigated and may result in disciplinary action up to and including dismissal from County employment. For violations of patient confidentiality, the procedures of the Patient Confidentiality Sanctions Policy as regulated by HIPAA will apply. Vendors who violate this policy may be subject to contract termination, denial of service, and/or legal penalties, both criminal and civil.

21.10. Revision History

Effective Date	**Changes Made**

7/31/2018	Policy established
6/22/2020	Policy revised

22. Additional Technology Terms and Conditions

22.1. Disentanglement

During the term of the Agreement and for a period of thirty (30) days following expiration or termination, Contractor shall make available an application programming interface ("API") that permits County to retrieve its Customer Data from the Contractor platform. Customer Data shall be provided in a non-proprietary format.

At County's written request, Contractor may extend API access to third-party contractors designated by County, provided that County remains solely responsible for vetting, authorizing, and managing such third parties. Contractor shall have no responsibility or liability for the acts or omissions of any third-party contractor and shall have no obligation to provide support or services directly to such third parties.

Except as expressly stated in this Section, Contractor shall have no obligation to provide transition assistance, data migration services, or other disengagement support. Any post-termination data retention, API access, maintenance, or support services shall be provided only pursuant to a mutually executed written agreement.

County must notify Contractor in writing at least thirty (30) days prior to expiration or termination of its intent to maintain data access or retention beyond the access period. Absent such notice and agreement, Contractor may delete Customer Data in accordance with its standard data retention and deletion policies.

Warranty

Contractor represents and warrants that, during the term of the Agreement, the services will be performed in a professional and workmanlike manner consistent with generally accepted industry standards and will substantially conform to the applicable documentation provided by Contractor.

County's sole and exclusive remedy for any breach of this warranty shall be for Contractor, at its option, to (a) use commercially reasonable efforts to correct the nonconformity, or (b) if Contractor determines that such correction is not commercially reasonable, refund the fees paid by County for the affected services for the period in which the nonconformity occurred.

The foregoing warranty does not apply to issues arising from (i) misuse of the services, (ii) modifications not made by or at the direction of Contractor, or (iii) use of the services in combination with products or services not provided by Contractor.

EXCEPT AS EXPRESSLY SET FORTH IN THIS SECTION, CONTRACTOR DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT.

23. Health Insurance Portability and Accountability Act (HIPAA)

23.1. DEFINITIONS

Terms used, but not otherwise defined, in this Schedule shall have the same meaning as those terms are defined in 45 Code of Federal Regulations (CFR) sections 160.103, 164.304, and 164.501. All regulatory references in this Schedule are to Title 45 of the Code of Federal Regulations unless otherwise specified.

a. ***Business Associate.*** "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the parties to this agreement shall mean Contractor.

b. ***Covered Entity.*** "Covered entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement shall mean County.

c. **HIPAA Rules**. "HIPAA rules" shall mean the Privacy, Security, Breach Notification and Enforcement Rules at 45 CFR part 160 and part 164, as amended and supplemented by Subtitle D of the Health Information Technology for Economic and Clinical Health Act provisions of the American Recovery and Reinvestment Act of 2009.

d. ***Designated Record Set***. "Designated Record Set" shall have the same meaning as the term "designated record set" in Section 164.501.

e. ***Electronic Protected Health Information***. "Electronic Protected Health Information" (EPHI) means individually identifiable health information that is transmitted or maintained in electronic media; it is limited to the information created, received, maintained or transmitted by Business Associate from or on behalf of Covered Entity.

f. ***Individual***. "Individual" shall have the same meaning as the term "individual" inSection 164.501 and shall include a person who qualifies as a personal representative in accordance with Section 164.502(g).

g. ***Privacy Rule***. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E. h. ***Protected Health Information***. "Protected Health Information" (PHI) shall have the same meaning as the term

"protected health information" in Section 160.103 and is limited to the information created or received by Business Associate from or on behalf of County.

i. ***Required By Law***. "Required by law" shall have the same meaning as the term "required by law" in Section 164.103.

j. ***Secretary***. "Secretary" shall mean the Secretary of the United States Department of Health and Human Services or his or her designee.

k. ***Breach***. The acquisition, access, use, or disclosure of PHI in violation of the Privacy Rule that compromises the security or privacy of the PHI and subject to the exclusions set forth in Section 164.402. Unless an exception applies, an impermissible use or disclosure of PHI *is presumed* to be a breach, unless it can be demonstrated there is a low probability that the PHI has been compromised based upon, at minimum, a four-part risk assessment:

> 1. Nature and extent of PHI included, identifiers and likelihood of re-identification; 2. Identity of the unauthorized person or to whom impermissible disclosure was made; 3. Whether PHI was actually viewed or only the opportunity to do so existed; 4. The extent to which the risk has been mitigated.

l. ***Security Rule***. "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 160 and Part 164, Subparts A and C.

m. ***Unsecured PHI.*** "Unsecured PHI" is protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in relevant HHS guidance.

n. ***Security Incident***. "Security Incident" shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system. "Security Incident" includes all incidents that constitute breaches of unsecured protected health information.

23.2. OBLIGATIONS AND ACTIVITIES OF CONTRACTOR AS BUSINESS ASSOCIATE

a. Business Associate agrees to not use or further disclose Protected Health Information other than as permitted or required by the Agreement or as required by law.

b. Business Associate agrees to use appropriate safeguards to comply with Subpart C of 45 CFR part 164 with respect to EPHI and PHI, and to prevent the use or disclosure of the Protected Health Information other than as provided for by this Agreement.

c. Business Associate agrees to make uses and disclosures requests for ProtectedHealth Information consistent with minimum necessary policy and procedures.

d. Business Associate may not use or disclose protected health information in a manner that would violate subpart E of 45 CFR part 164.504 if used or disclosed by Covered Entity.

e. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

f. Business Associate agrees to report to County any use or disclosure of Protected Health Information not authorized by this Agreement.

g. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of County, agrees to adhere to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

h. If Business Associate has Protected Health Information in a Designated Record Set, Business Associate agrees to provide access, at the request of County, and in the time and manner designated by County, to Protected Health Information in a Designated Record Set, to County or, as directed by County, to an Individual in order to meet the requirements under Section 164.524.

i. If Business Associate has Protected Health Information in a Designated Record Set, Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the County directs or agrees to make pursuant to Section 164.526 at the request of County or an Individual, and in the time and manner designed by County.

j. Business Associate agrees to make available to the Secretary of the United States Department of Health and Human Services, and to County upon reasonable prior written request, such records relating to Business Associate's use and disclosure of Protected Health Information on behalf of County as are reasonably necessary to demonstrate County's compliance with the HIPAA Rules. Any access by County under this Section shall be limited in scope to records directly relevant to such compliance, shall be conducted in a manner that does not unreasonably interfere with Business Associate's operations, and shall be subject to reasonable confidentiality protections. Business Associate shall not be required to disclose trade secrets, proprietary information, internal security architecture, or information unrelated to the use or disclosure of Protected Health Information.

k. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for County to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with Section 164.528.

l. Business Associate agrees to provide to County or an Individual in the time and manner designated by County, information collected in accordance with Section (k) of this Schedule, in order to permit County to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with Section 164.528.

m. Business Associate shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of EPHI that Business Associate creates, receives, maintains, or transmits on behalf of County.

n. Business Associate shall conform to generally accepted system security principles and the requirements of the final HIPAA rule pertaining to the security of health information.

o. Business Associate shall ensure that any agent to whom it provides EPHI, including a subcontractor, agrees to implement reasonable and appropriate safeguards to protect such EPHI.

p. Business Associate shall report to County Breach of Unsecured PHI without unreasonable delay and within three (3) business days of becoming aware of such incident. Business Associate shall also facilitate breach notification(s) to the appropriate governing body (i.e. HHS,OCR, etc.) as required by law. As appropriate and after consulting with County, Business Associate shall also notify affected individuals and the media of a qualifying breach. Non-Breach incidents may be reported on a periodic basis.

q. Business Associate understands that it is directly liable under the HIPAA rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of Protected Health Information that are not authorized by this Attachment, the underlying contract as or required by law.

23.3. PERMITTED USES AND DISCLOSURES BY CONTRACTOR AS BUSINESS ASSOCIATE

Except as otherwise limited in this Schedule, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, County as specified in the Agreement; provided that such use or disclosure would not violate the Privacy Rule if done by County.

23.4. OBLIGATIONS OF COUNTY

a. County shall provide Business Associate with the notice of privacy practices that County produces in accordance with Section 164.520, as well as any changes to such notice.

b. County shall provide Business Associate with any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, if such changes affect Business Associate's permitted or required uses and disclosures.

c. County shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that County has agreed to in accordance with Section 164.522.

23.5. PERMISSIBLE REQUESTS BY COUNTY

County shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if so requested by County, unless the Business Associate will use or disclose Protected Health Information for, and if the Agreement provides for, data aggregation or management and administrative activities of Business Associate.

23.6. DUTIES UPON TERMINATION OF AGREEMENT

a. Upon termination of the Agreement for any reason, Business Associate shall, at County's direction, return or destroy all Protected Health Information received from County, or created, received, or maintained by Business Associate on behalf of County, that Business Associate maintains in active systems. This obligation shall apply to Protected Health Information in the possession of Business Associate's subcontractors or agents.

Notwithstanding the foregoing, Business Associate may retain Protected Health Information in secure backups, disaster recovery systems, or archival media to the extent such retention is reasonably necessary for legal, regulatory, or business continuity purposes, provided that such retained information remains subject to the protections of this Agreement and is not used or disclosed for any purpose other than those that make such retention necessary. Business

Associate shall destroy such retained Protected Health Information in accordance with its standard data retention and deletion policies.

b. In the event that Business Associate determines that returning or destroying Protected Health Information is infeasible, Business Associate shall provide to County notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of the Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protection Health Information.

23.7. MISCELLANEOUS

a. **Regulatory References**. A reference in this Schedule to a section in the HIPAA Privacy Rule means the section as in effect or as amended, and for which compliance is required.

b. **Amendment**. The Parties agree to take such action as is necessary to amend this Schedule from time to time as is necessary for County to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act, Public Law 104-191.

c. **Survival**. The respective rights and obligations of Business Associate under this Schedule shall survive the termination of the Agreement.

d. **Interpretation**. [DELETED]

e. **Reservation of Right to Monitor Activities**. County may, upon reasonable prior written notice and no more than once annually, request information reasonably necessary to confirm Business Associate's compliance with the HIPAA Security Rule as it relates to the protection of Protected Health Information on behalf of County. Any such review shall be limited in scope, shall not unreasonably interfere with Business Associate's operations, and shall be subject to reasonable confidentiality obligations. County shall not be entitled to conduct on-site inspections, penetration testing, or vulnerability scanning, or to access Business Associate's internal security architecture, source code, or other proprietary or confidential information.

24. Intellectual Property

24.1. Intellectual Property Rights

1. The County of San Mateo ("County"), shall and does own all titles, rights and interests in all Work Products created by Contractor and its subcontractors (collectively "Vendors") for the County under this Agreement. Contractor may not sell, transfer, or permit the use of any Work Products without the express written consent of the County.

2. "Work Products" are defined as all materials, tangible or not, created in whatever medium pursuant to this Agreement, including without limitation publications, promotional or educational materials, reports, manuals, specifications, drawings and sketches, computer programs, software and databases, schematics, marks, logos, graphic designs, notes, matters and combinations thereof, and all forms of intellectual property.

3. Contractor shall not dispute or contest, directly or indirectly, the County's exclusive right and title to the Work Products nor the validity of the intellectual property embodied therein.

Contractor hereby assigns, and if later required by the County, shall assign to the County all titles, rights and interests in all Work Products. Contractor shall cooperate and cause subcontractors to cooperate in perfecting County's titles, rights or interests in any Work Product, including prompt execution of documents as presented by the County.

4. To the extent any of the Work Products may be protected by U.S. Copyright laws, Parties agree that the County commissions Vendors to create the copyrightable Work Products, which are intended to be work-made-for-hire for the sole benefit of the County and the copyright of which is vested in the County.

5. In the event that the title, rights, and/or interests in any Work Products are deemed not to be "work-made-for-hire" or not owned by the County, Contractor hereby assigns and shall require all persons performing work pursuant to this Agreement, including its subcontractors, to assign to the County all titles, rights, interests, and/or copyrights in such Work Product. Should such assignment and/or transfer become necessary or if at any time the County requests cooperation of Contractor to perfect the County's titles, rights or interests in any Work Product, Contractor agrees to promptly execute and to obtain execution of any documents (including assignments) required to perfect the titles, rights, and interests of the County in the Work Products with no additional charges to the County beyond that identified in this Agreement or subsequent change orders. The County, however, shall pay all filing fees required for the assignment, transfer, recording, and/or application.

6. Contractor agrees that before commencement of any subcontract work it will incorporate this **SECTION** to contractually bind or otherwise oblige its subcontractors and personnel performing work under this Agreement such that the County's titles, rights, and interests in Work Products are preserved and protected as intended herein.

25. Personally Identifiable Information

Requirements for County Contractors, Subcontractors, Vendors and Agents

25.1. Definitions

Personally Identifiable Information (PII), or Sensitive Personal Information (SPI), as used in Federal information security and privacy laws, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. PII may only be used to assist in the administration of programs in accordance with 45 C.F.R. § 205.40, *et seq*. and California Welfare & Institutions Code section 10850.

a. **"Assist in the Administration of the Program"** means performing administrative functions on behalf of County programs, such as determining eligibility for, or enrollment in, and collecting context PII for such purposes, to the extent such activities are authorized by law.

b. **"Breach"** refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to context PII, whether electronic, paper, verbal, or recorded.

c. **"Contractor"** means those contractors, subcontractors, vendors and agents of the County performing any functions for the County that require access to and/or use of PII and that are authorized by the County to access and use PII.

d. **"Personally Identifiable Information" or "PII"** is personally identifiable information that can be used alone, or in conjunction with any other reasonably available information, to identify a specific individual. PII includes, but is not limited to, an individual's name, social security number, driver's license number, identification number, biometric records, date of birth, place of birth, or mother's maiden name. PII may be electronic, paper, verbal, or recorded.

e. **"Security Incident"** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PII, or interference with system operations in an information system which processes PII that is under the control of the County or County's Statewide Automated Welfare System (SAWS) Consortium, or under the control of a contractor, subcontractor or vendor of the County, on behalf of the County.

f. "**Secure Areas**" means any area where:

i. Contractors administer or assist in the administration of County programs; ii. PII is used or disclosed; or

iii. PII is stored in paper or electronic format.

25.2. Restrictions on Contractor re Use and Disclosure of PII

a. Contractor agrees to use or disclose PII only as permitted in this Agreement and only to assist in the administration of programs in accordance with 45 CFR § 205.50, *et seq*. and California Welfare & Institutions Code section 10850 or as otherwise authorized or required by law. Disclosures, when authorized or required by law, such as in response to a court order, or when made upon the explicit written authorization of the individual, who is the subject of the PII, are allowable. Any other use or disclosure of PII requires the express approval in writing by the County. No Contractor shall duplicate, disseminate or disclose PII except as allowed in this Agreement.

b. Contractor agrees to only use PII to perform administrative functions related to the administration of County programs to the extent applicable.

c. Contractor agrees that access to PII shall be restricted to Contractor's staff who need to perform specific services in the administration of County programs as described in this Agreement.

d. Contractor understands and agrees that any of its staff who accesses, discloses or uses PII in a manner or for a purpose not authorized by this Agreement may be subject to civil and criminal sanctions available under applicable Federal and State laws and regulations

25.3. Use of Safeguards by Contractor to Protect PII

a. Contractor agrees to ensure that any agent, including a subcontractor, to whom it provides PII received from, or created or received by Contractor on behalf of County, agrees to adhere to the same restrictions and conditions contained in this Attachment PII.

b. Contractor agrees to advise its staff who have access to PII, of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in applicable Federal and State laws and regulations.

The physical handling, mailing, faxing, and transport requirements set forth in this Section apply only to the extent Contractor processes or stores PII in physical (paper) form.

c. Contractor agrees to train and use reasonable measures to ensure compliance by Contractor's staff, including, but not limited to (1) providing initial privacy and security awareness training to each new staff within thirty (30) days of employment; (2) thereafter, providing annual refresher training or reminders of the PII privacy and security safeguards to all Contractor's staff; (3) maintaining records indicating each Contractor's staff name and the date on which the privacy and security awareness training was completed; and (4) retaining training records for a period of three (3) years after completion of the training or equivalent documentation maintained in accordance with Contractor's standard training and compliance practices.

d. Contractor agrees to provide documented sanction policies and procedures for Contractor's staff who fail to comply with privacy policies and procedures or any provisions of these requirements, including termination of employment when appropriate.

e. Contractor agrees that all Contractor's staff performing services under this Agreement sign a confidentiality statement prior to accessing PII and . The signed statement shall be retained for a period of three (3) years, and the statement include at a minimum: (1) general use; (2) security and privacy safeguards; (3) unacceptable use; and (4) enforcement policies.

f. Contractor agrees to conduct a background check of Contractor's staff before they may access PII with more thorough screening done for those employees who are authorized to bypass significant technical and operational security controls. Contractor further agrees that screening documentation shall be retained for a period of three (3) years following conclusion of the employment relationship consistent with applicable law and Contractor's internal employment and background screening policies.

g. Contractor agrees to conduct periodic privacy and security reviews of work activity, including random sampling of work product by Contractor's staff by management level personnel who are knowledgeable and experienced in the areas of privacy and information security in the administration of County's programs and the use and disclosure of PII. Examples include, but are not limited to, access to data, case files or other activities related to the handling of PII.

h. Contractor shall ensure that PII is used and stored in an area that is physically safe from access by unauthorized persons at all times and safeguard PII from loss, theft, or inadvertent disclosure by securing all areas of its facilities where Contractor's staff assist in the administration of the County's programs and use, disclose, or store PII.

Notwithstanding anything to the contrary in this Section, to the extent Contractor utilizes third-party cloud service providers to host, process, or store PII, Contractor's obligations with respect to physical and environmental security controls shall be satisfied through the security, access controls, and certifications of such cloud service providers, provided that such providers maintain industry-standard security practices consistent with generally accepted frameworks such as SOC 2, ISO 27001, or NIST SP 800-53.

i. Contractor shall ensure that each physical location, where PII is used, disclosed, or stored, has procedures and controls that ensure an individual who is terminated from access to the facility is promptly escorted from the facility by an authorized employee of Contractor and access is revoked.

j. Contractor shall ensure that there are security guards or a monitored alarm system at all times at Contractor's facilities and leased facilities where five hundred (500) or more individually identifiable records of PII is used, disclosed, or stored. Video surveillance systems are recommended.

k. Contractor shall ensure that data centers with servers, data storage devices, and/or critical network infrastructure involved in the use, storage, and/or processing of PII have perimeter security and physical access controls that limit access to only those authorized by this Agreement. Visitors to any Contractor data centers area storing PII as a result of administration of a County program must be escorted at all times by authorized Contractor's staff.

l. Contractor shall have policies that include, based on applicable risk factors, a description of the circumstances under which Contractor staff can transport PII, as well as the physical security requirements during transport.

m. Contractor shall ensure that any PII stored in a vehicle shall be in a non-visible area such as a trunk, that the vehicle is locked, and under no circumstances permit PII be left unattended in a vehicle overnight or for other extended periods of time.

n. Contractor shall ensure that PII shall not be left unattended at any time in airplanes, buses, trains, etc., including baggage areas. This should be included in training due to the nature of the risk.

o. Contractor shall ensure that all workstations and laptops, which use, store and/or process PII, must be encrypted using a FIPS 140-2 certified algorithm 128 bit or higher, such as Advanced Encryption Standard (AES). The encryption solution must be full disk. It is encouraged, when available and when feasible, that the encryption be 256 bit.

p. Contractor shall ensure that servers containing unencrypted PII must have sufficient administrative, physical, and technical controls in place to protect that data, based upon a risk assessment/system security review. It is recommended to follow the guidelines documented in the latest revision of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

q. Contractor agrees that only the minimum necessary amount of PII required to perform required business functions will be accessed, copied, downloaded, or exported.

r. Contractor shall ensure that all electronic files, which contain PII data is encrypted when stored on any mobile device or removable media (i.e. USB drives, CD/DVD, smartphones, tablets, backup tapes etc.). Encryption must be a FIPS 140-2 certified algorithm 128 bit or higher, such as AES. It is encouraged, when available and when feasible, that the encryption be 256 bit.

s. Contractor shall ensure that all workstations, laptops and other systems, which process and/or store PII, must install and actively use an antivirus software olution. Antivirus software should have automatic updates for definitions scheduled at least daily. In addition, Contractor shall ensure that:

i. All workstations, laptops and other systems, which process and/or store PII, must have critical security patches applied, with system reboot if necessary.

ii. There must be a documented patch management process that determines installation timeframe based on risk assessment and vendor recommendations.

iii. At a maximum, all applicable patches deemed as critical must be installed within thirty (30) days of vendor release. It is recommended that critical patches which are high risk be installed within seven (7) days.

iv. Applications and systems that cannot be patched within this time frame, due to significant operational reasons, must have compensatory controls implemented to minimize risk.

t. Contractor shall implement reasonable and appropriate authentication and session management controls designed to protect PII, consistent with generally accepted industry standards and Contractor's written security policies, taking into account applicable risk factors and evolving best practices.

u. Contractor shall ensure that usernames for its staff authorized to access PII will be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee within twenty- four (24) hours. Note: Twenty-four (24) hours is defined as one (1) working day.

v. Contractor shall ensure when no longer needed, all PII must be cleared, purged, or destroyed consistent with NIST SP 800-88, Guidelines for Media Sanitization, such that the Personally Identifiable Information cannot be retrieved.

w. Contractor shall implement reasonable and appropriate authentication and session management controls designed to protect PII, consistent with generally accepted industry standards and Contractor's written security policies, taking into account applicable risk factors and evolving best practices.

x. Contractor shall ensure that all of its systems providing access to PII must display a warning banner stating, at a minimum that data is confidential; systems are logged, systems use is for business purposes only by authorized users and users shall log off the system immediately if they do not agree with these requirements.

y. Contractor will ensure that all of its systems providing access to PII must maintain an automated audit trail that can identify the user or system process which initiates a request for PII, or alters PII. The audit trail shall be date and time stamped; log both successful and failed accesses be read-access only; and be restricted to authorized users. If PII is stored in a database, database logging functionality shall be enabled. The audit trail data shall be archived for at least one (1) year from the occurrence.

z. Contractor shall ensure that all of its systems providing access to PII shall use role-based access controls for all user authentications, enforcing the principle of least privilege.

aa. Contractor shall ensure that all data transmissions of PII outside of its secure internal networks must be encrypted using a Federal Information Processing Standard (FIPS) 140-2 certified algorithm that is 128 bit or higher, such as Advanced Encryption Standard (AES) or Transport Layer Security (TLS). It is encouraged, when available and when feasible, that 256 bit encryption be used. Encryption can be end to end at the network level, or the data files containing PII can be encrypted. This requirement pertains to any type of PII in motion such as website access, file transfer, and email.

bb. Contractor shall ensure that all of its systems involved in accessing, storing, transporting, and protecting PII, which are accessible through the Internet, must be protected by an intrusion detection and prevention solution.

cc. Contractor shall ensure that audit control mechanisms are in place. All Contractor systems processing and/or storing Personally Identifiable Information must have a least an annual system risk assessment/security review that ensure administrative, physical, and technical controls are functioning effectively and provide an adequate level of protection. Review shall include vulnerability scanning tools.

dd. Contractor shall ensure that all of its systems processing and/or storing PII must have a process or automated procedure in place to review system logs for unauthorized access.

ee. Contractor shall ensure that all of its systems processing and/or storing PII must have a documented change control process that ensures separation of duties and protects the confidentiality, integrity and availability of data.

ff. Contractor shall establish a documented plan to enable continuation of critical business processes and protection of the security of PII kept in an electronic format in the event of an emergency. Emergency means any circumstance or situation that causes normal computer operations to become unavailable for use in performing the work required under this Agreement for more than twenty-four (24) hours.

gg. Contractor shall ensure its data centers with servers, data storage devices, and critical network infrastructure involved in the use, storage and/or processing of PII, must include environmental protection such as cooling, power, and fire prevention, detection, and suppression.

hh. Contractor shall establish documented procedures to backup PII to maintain retrievable exact copies of PIII. The documented backup procedures shall contain a schedule which includes incremental and full backups, storing backups offsite, inventory of backup media, recovery of PII data, an estimate of the amount of time needed to restore PII data.

ii. Contractor shall ensure that PII in paper form shall not be left unattended at any time, unless it is locked space such as a file cabinet, file room, desk or office. Unattended means that information may be observed by an individual not authorized to access the information. Locked spaces are defined as locked file abinets, locked file rooms, locked desks, or locked offices in facilities which are multi-use, meaning that there are Contractor's staff and non-Contractor functions in one building in work areas that are not securely segregated from each other. It is recommended that all PII be locked up when unattended at any time, not just within multi-use facilities.

jj. Contractor shall ensure that any PII that must be disposed of will be through confidential means, such as crosscut shredding or pulverizing.

kk. Contractor agrees that PII must not be removed from its facilities except for identified routine business purposes or with express written permission of the County.

ll. Contractor shall ensure that faxes containing PII shall not be left unattended and fax machines shall be in secure areas. Faxes containing PII shall contain a confidentiality statement

notifying persons receiving faxes in error to destroy them and notify the sender. All fax numbers shall be verified with the intended recipient before send the fax.

mm. Contractor shall ensure that mailings containing PII shall be sealed and secured from damage or inappropriate viewing of PII to the extent possible. Mailings that include five hundred (500) or more individually identifiable records containing PII in a single package shall be sent using a tracked mailing method that includes verification of delivery.

25.4. Reporting of Breaches Required by Contractor to County; Mitigation

a. Contractor shall notify County without unreasonable delay, and in no event later than five (5) business days, after confirming a Breach of unsecured PII as defined by applicable law. Contractor may provide periodic or aggregated reporting of non-breach security incidents upon County's reasonable request.

b. Contractor understands that State and Federal Law requires a breaching entity to notify individuals of a breach or unauthorized disclosure of their PII. Contractor shall ensure that said notifications shall comply with the requirements set forth in California Civil Code section 1798.29, and 42 U.S.C. section 17932, and its implementing regulations, including but not limited to, the requirement that the notifications be made without unreasonable delay and in no event later than sixty (60) calendar days.

c. Contractor agrees to promptly mitigate, to the extent practicable, any harmful effect that is known to Contractor stemming from a use or disclosure of PII in violation of the requirements of this Agreement, including taking any action pertaining to such use or disclosure required by applicable Federal and State laws and regulations.

25.5. Permitted Uses and Disclosures of PII by Contractor

Except as otherwise limited in this schedule, Contractor may use or disclose PII to perform functions, activities, or services for, or on behalf of, County as specified in the Agreement; provided that such use or disclosure would not violate the Privacy Rule if done by County.

25.6. Obligations of County

a. County shall provide Contractor with the notice of privacy practices that County produces in accordance with California Welfare and Institutions Code section 0850, as well as any changes to such notice.

b. County shall notify Contractor of any changes in, or revocation of, permission by Individual to use or disclose PII, if such changes affect Contractor's permitted or required uses and disclosures.

c. County shall notify Contractor of any restriction to the use or disclosure of PII that County has agreed to in accordance with California Welfare and Institutions Code section 10850.

25.7. Permissible Requests by County

County shall not request Contractor to use or disclose PII in any manner that would not be permissible under the Privacy Rule if so requested by County, unless Contractor will use or disclose PII for, and if the Agreement provides for, data aggregation or management and administrative activities of Contractor.

25.8. Duties Upon Termination of Agreement

a. Upon termination of the Agreement for any reason, Contractor shall return or destroy all PII maintained in active systems that was received from County or created, maintained, or received by Contractor on behalf of County. Notwithstanding the foregoing, Contractor may retain PII in secure backups, disaster recovery systems, or archival media to the extent reasonably necessary for legal, regulatory, or business continuity purposes, provided such PII remains subject to the protections of this Agreement and is destroyed in accordance with Contractor's standard data retention policies.

b. In the event that Contractor determines that returning or destroying PII is infeasible, Contractor shall provide to County notification of the conditions that make return or destruction infeasible. The Parties acknowledge that such conditions may include, without limitation, Contractor's obligation to retain certain information for compliance purposes (including audit logs) and Contractor's use of data related to use of the platform for internal product improvement, analytics, and security purposes, as described in Contractor's platform privacy policy. Upon mutual Agreement of the Parties that return or destruction of PII is infeasible, Contractor shall extend the protections of the Agreement to such PII and limit further uses and disclosures of such PII to those purposes that make the return or destruction infeasible, provided that such use does not identify the County or individual data subjects, for so long as Contractor maintains such PII.

25.9. Miscellaneous

a. **Regulatory References.** A reference in this Attachment to a section in the Personally Identifiable Information Privacy Rule means the section as in effect or as amended, and for which compliance is required.

b. **Amendment.** The Parties agree to take such action as is necessary to amend this Schedule from time to time as is necessary for County to comply with the requirements of the Privacy Rule and in accordance 45 CFR § 205.40, *et seq*. and California Welfare and Institutions Code section 10850.

c. **Survival.** The respective rights and obligations of Contractor under this Attachment shall survive the termination of the Agreement unless and until the PII is destroyed or returned to the County.

d. **Interpretation.** Any ambiguity in this Attachment shall be interpreted in a manner consistent with applicable law and the terms of the Agreement.

e. **Reservation of Right to Monitor Activities.** County may, upon reasonable prior written notice and no more than once annually, request information reasonably necessary to confirm Contractor's compliance with applicable PII protection requirements. Any such review shall be limited in scope, shall not unreasonably interfere with Contractor's operations, and shall not require disclosure of proprietary information, internal security architecture, or trade secrets.

26. Rehabilitation Act of 1973

Refer to the attachment required to be completed by the Contractor.

SIGNATURE PAGE TO FOLLOW

THIS PAGE INTENTIONALLY LEFT BLANK

In witness of and in agreement with this Agreement's terms, the parties, by their duly authorized representatives, affix their respective signatures:

For Contractor: Peregrine Technologies Inc

William R Wheeler William R Wheeler (Jan 22, 2026 09:22:31 PST)	01/22/26	William R Wheeler
Contractor Signature	Date	Contractor Name (please print)

COUNTY OF SAN MATEO

By:

President, Board of Supervisors, San Mateo County

Date:

ATTEST:

By:

Clerk of Said Board

EXHIBIT [A]: SERVICES

PEREGRINE STATEMENT OF WORK

Scope & Description of the Peregrine Service Applications

The Peregrine platform (the "Service," "Peregrine"), is a web-based, CJIS-compliant software-as-a-service (SaaS) that provides a single point of access to integrate, discover, view, and analyze data from the below-listed agencies ("Participating Agencies." Under this scope of work, Peregrine will integrate data from the following Participating Agency sources:

- San Mateo Police Department: CAD; RMS; Axon Evidence; Axon LPR; and Skydio
- South San Francisco Police Department: CAD; RMS; Axon Evidence; and Axon LPR
- Daly City Police Department: CAD; RMS; Axon Evidence; Axon LPR; and Skydio
- San Bruno Police Department: CAD; RMS; Axon Evidence; and Axon LPR
- Pacifica Police Department: CAD; RMS; Axon Evidence; and Axon LPR
- Redwood City Police Department: CAD; RMS; Axon Evidence; and Axon LPR
- Hillsborough Police Department: CAD; RMS; Axon Evidence; and Axon LPR
- Foster City Police Department: CAD; RMS; Axon Evidence; and Axon LPR
- Menlo Park Police Department: CAD; RMS; Axon Evidence; and Axon LPR
- Atherton Police Department: CAD; RMS; Axon Evidence; and Axon LPR
- Burlingame Police Department: CAD; RMS; Axon Evidence; and Axon LPR
- Belmont Police Department: CAD; RMS; Axon Evidence; and Axon LPR
- East Palo Alto Police Department: CAD; RMS; Axon Evidence; and Axon LPR
- Colma Police Department: CAD; RMS; Axon Evidence; and Axon LPR
- San Mateo County Sheriff's Office: CAD; RMS; Axon Evidence; Axon LPR; Jail Management System (JMS); and Flock ALPR
- San Mateo County District Attorney's Office: CAD; RMS; Axon Evidence; and Axon LPR
- Brisbane Police Department: CAD; RMS; Axon Evidence; and Axon LPR
- Broadmoor Police Department: CAD; RMS; Axon Evidence; and Axon LPR

For LPR data, this scope of work supports 30-day retention of detections and up to 20M annual detections per Participating Agency. For San Mateo County Sheriff's Office, this scope of work supports 30-day retention of detections and up to 100M LPR reads annually.

Peregrine is providing these capabilities under a firm-fixed-price license that includes all support, training, and cloud hosting services needed to achieve the project objectives. Additionally, this scope of work allows for an unlimited number of users from Participating Agencies to access and utilize Peregrine.

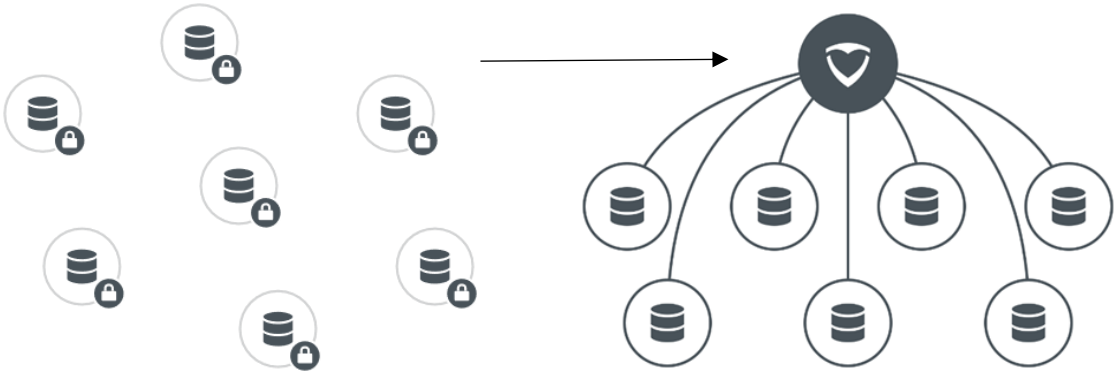
The platform performs several critical functions including data integration, search and information retrieval, advanced analytics, data management, reporting, data exchange and sharing, access control, audit logging, and security.

The Peregrine platform provides an efficient method for turning large amounts of raw data into actionable information. Peregrine does not provide nor create new data for its customers—our platform integrates existing data and makes it available to end users in a decision-ready state.

DATA INTEGRATION & MODELING

The Participating Agency has volumes of valuable data, but that value cannot be unlocked because data is scattered across separate systems, siloed in ways that prevent it from being understood and analyzed together. The Peregrine platform is built to rapidly integrate, clean, transform, and model large amounts of raw data from disparate systems and continuously surface actionable information while reducing manual processing needs.

Peregrine Unlocks Data Sources by Integrating Them into a Single, Secure Platform



The platform securely integrates data in near-real time to ensure that users have the most current and reliable information when and where they need it. As data flows into the platform, granular security controls, retention policies, and changes from underlying systems are continuously monitored and applied.

As soon as data enters the platform, it is mapped to an agency-specific data model that is molded to the unique operations of the Participating Agenc. This data model provides a dynamic representation of all data – entities, locations, events, and the links between them. Harmonizing multi-source data into one data model allows users to smoothly analyze data without requiring a technical understanding of the underlying source systems themselves.

The data model is a dynamic layer of the Peregrine platform, one that can evolve and adapt in response to changes in the Participating Agency's underlying data systems, even as those systems are upgraded or swapped out.

SEARCH & INFORMATION RETRIEVAL

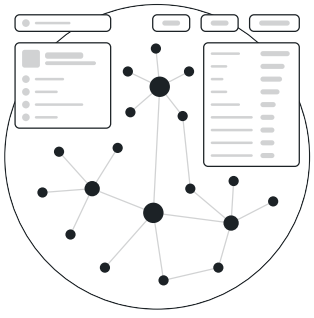
Once data is integrated into the Peregrine platform, it is immediately accessible through front-end applications. Personnel can easily search for data and filter based on criteria relevant for their investigations, analysis, or other workflow. The Peregrine platform is intuitive to use, allowing personnel of varying technical abilities, skillsets, and functions to surface information that is relevant to them and streamline their unique search workflows.

The platform is designed to be walk-up usable; new users of the platform can immediately surface, analyze, and action data by navigating the platform's intuitive user interface and applications. These users have multiple ways to surface and view relevant information, allowing them flexibility to approach questions and decisions in ways that best suit them. These features mean that users arrive at answers more quickly and with greater accuracy, saving time and effort.

EXPLORATION, VISUALIZATION, & REPORTING TOOLS

The Peregrine platform provides a powerful suite of tools for the exploration, visualization, and reporting of data. These tools enable personnel to create dynamic data products and reports—such as interactive maps, network graphs, and dashboards—that automatically update as new data flows into the platform. Personnel can smoothly move data between analytical tools, viewing the same data in different modalities without having to log into different systems or applications. The following subsections provide more information regarding these analysis tools.

Geospatial Analysis Tool. To better understand geographical assets, events, and trends, the Peregrine platform includes an interactive Map application. The Map allows users to conduct visually intuitive geographical analysis on all agency data, both historical and in real-time. Users can surface trends, make connections, filter to areas of interest, drill into specific events, particular time periods, and add new layers of relevance on top as needed. The Map is designed for next-generation geographic contextual and situational awareness, allowing users to explore and answer specific questions with the most relevant data. The Map is intuitive for all personnel whether they are consuming pre-built analyses, conducting ad-hoc searches, or creating complex geospatial products from scratch.



Link Chart Analysis Tool. The platform's Link Chart aids in the discovery and visualization of connections between otherwise disconnected data. The Link Chart allows users to discover links between people, places, entities, and events across one or multiple degrees of separation. Peregrine's platform also automatically extracts links from both structured and unstructured data to illuminate connections between people, places, events, documents, and media data without requiring manual processing. For example, an address written in narrative form within a scanned document can be automatically linked to a person living at that address or to a vehicle registered there.

Reports & Dashboards. The platform's report and dashboard applications provide configurable, real-time executive summaries to inform situational awareness, statistical analysis, and decision making. Reports and dashboards are configurable to meet the unique needs and visual preferences of individual users. All reports and dashboards are directly connected to real-time data feeds, empowering users to drill down from high-level summary information to the most granular context with a single click. Once a user creates a dashboard, they can continue to use it indefinitely—and share it as needed.

Temporal Analysis Tool. By centralizing data—and all associated metadata—from data systems, users can understand and surface trends over time. Through an intuitive interface, users can analyze how, e.g., calls for service or types of incidents vary by day of week and time of day. Peregrine supports robust search and query capabilities at the day of week and hour of day level, enabling users to conduct analysis over specific units, in specific shifts, at specific locations. As a result, organization can make more informed, data-backed resourcing decisions to more effectively meet mission outcomes.

Real-Time Alerting. With all data centrally located, users can receive real-time notification on new data from any source system. The Peregrine platform's alerting technology can notify specific users if a pre-defined data entity was added or removed, viewed, downloaded, renamed, or shared. This includes geo-fenced areas or user-defined polygons. For instance, if a neighborhood is experiencing a trend in a type of crime, a Peregrine user can create an alert through the platform's "follow" feature. If another similar crime occurs in the defined area, a real-time notification will be sent to all users following this alert via email, SMS, or both.

Mobile Application.

The Peregrine Mobile application has many of the same capabilities as our web-based platform and includes the ability to: search across siloed data systems; rapidly visualize and analyze data with a variety of analytical tools (maps, tables, etc.), and send information between personnel and teams, and configure custom alerts. Peregrine's Mobile application is protected through two-factor authentication, including biometric authentication, and all data in the application is fully secured and encrypted to ensure CJIS compliance. This Mobile application is available on both iOS and Android devices.

Permission-based Collaboration & Sharing

The Peregrine platform provides features for secure collaboration and sharing that will enable the Participating Agency to build deeper, trusting partnerships with local and regional stakeholders, including with County of San Mateo leadership and the broader community. The platform's granular access and usage control capabilities prevent unauthorized or inappropriate use or sharing of sensitive data while allowing agencies and departments to share information with their partners in a deliberate, precise, and auditable manner.

Collaboration in the Peregrine platform extends beyond simple data sharing; it also allows for multiple users to work within the same application at the same time across multiple devices and locations. The platform's collaboration features compound the value of users' work by dynamically connecting them in real time with other users who are working with or interested in the same data. In this way, the Peregrine platform generates opportunities for users to improve the quality and speed of their answers by connecting them to users who are asking the same question.

Peregrine's collaboration features will allow Participating Agency users to share information available in Peregrine with authorized external users (e.g., other neighboring law enforcement agencies) even if those users' organizations do not have their own Peregrine software licenses.

Implementation and Delivery Methodology

Peregrine engages with our customer via fixed-price, annual licenses. A Customer's license includes all needed implementation and delivery support to achieve project objectives.

Implementation team. Peregrine implementation teams consist of software engineering, product development, human-centered design, user engagement, and training experts. The Peregrine implementation team will provide the Customer continuous support and collaborate closely with the Customer to provide use case development, data modeling, data integration, training curriculums, use case / workflow development, and continuous support. This team is committed to ensure that the Peregrine platform is quickly deployed, securely configured, and adopted for its intended purpose.

Solution Timeline & Implementation Model. Each Peregrine platform implementation consists of four steps to maximize success and impact at the outset of our partnership. These steps typically enable implementation and use within 90 days.*

Milestone	Delivery	Deliverable
1 – Kickoff and Scoping	Week 2	1. Determine priority order of data integrations and user groups 2. Facilitate Peregrine team access to data sources and initial users 3. Set up project team and steering committee
2 – Data Integration, Data Modeling, and User Discovery	Month 1	1. Deploy the Peregrine platform 2. Ingest, integrate, transform, model, and validate data sources 3. Configure permission controls 4. Introduce platform to the first set of users 5. Conduct 45-day steering committee review
3 – Real-time Workflows and Analytics	Month 2	1. Initiate user training 2. Develop and implement user and team-specific workflows
4 – Operationalization and Next Steps	Month 3	1. Continue collecting feedback and improve user workflows 2. Validate work based on actionable results 3. Identify next steps 4. Conduct 90-day steering committee review (quarterly thereafter)

** Integration timelines provided are from date of access to relevant networks and data sources.*

Peregrine's implementation team will work with Participating Agency to get access to appropriate networks and data sources in a timely manner and requires support from the Customer to facilitate such access.

Required Assistance from Customer IT. Under this scope of work, Peregrine will be integrating sources of information that are hosted on premises within Participating Agency's network and sources that are third-party, cloud hosted systems. Peregrine requests the following support from Participating Agency's IT. The methods outlined below are Peregrine's preferred methods of connecting to relevant networks and systems. Should any of those methods be unavailable, Peregrine will work with Participating Agency's IT to determine the most efficient and effective methods to allow for data access.

- Enable access to Participating Agency's network by, among other things, enabling an IPSec tunnel that enables Peregrine's access to necessary systems hosted within Participating Agency's network;
- enable access to Participating Agency's identity and access management (IDAM) solution in order to enable synchronization with Participating Agency's login credentials;

- provide read-only accounts to all in-scope Participating Agency-managed and hosted systems (e.g., RMS, CAD)
- provide or facilitate the provision to accounts to all in-scope third-party managed and hosted systems (e.g., Evidence.com, Flock)

Support Methodology

Peregrine provides ongoing support to the Customer on a 24x7x365 basis as part of the annual term license. The Peregrine platform includes an integrated support feature by which users can file support issues or ask questions. Additionally, self-help user guides are available in the Peregrine Knowledge Base, designed to answer frequently asked questions and provide walk through guides of common workflows.

System Availability

During any calendar month, the Peregrine system shall be available to users no less than 99.9% of the time on a 24x7 basis, excluding scheduled maintenance of the system, provided that Peregrine is not responsible for any downtime of the applications or software caused by third party data services (e.g., RMS databases). Peregrine shall provide prompt notification as soon as it becomes aware of any actual or potential unscheduled downtime of the system, as well as periodic updates during the unscheduled downtime regarding Peregrine's progress in remedying the unavailability and the estimated time at which the system shall be available.

Issue Response and Resolution

Severity Level	Level of Effort	Initial Response	Work Around	Targeted Time to Permanent Fix	Status Updates
1	Continuous best efforts, 24/7	Immediate, but in no event to exceed 30 minutes	8 hours	3 calendar days	Every 2 hours prior to work around and every calendar day until permanent correction
2	Commercially reasonable efforts, 24/7	1 hour	24 hours	5 calendar days	Every 6 hours prior to work around and every calendar day until permanent correction
3	Commercially reasonable efforts, during normal business hours	1 business day	10 business days	20 business days	Every 2 business days prior to work around and every calendar day until permanent correction

- **"Severity level 1 error"** means any system error that, for fifty percent (50%) or more of Participating Agency's users, renders the system or any material portion of the system inoperative, or materially impairs use of the system in a production environment.
- **"Severity level 2 error"** means any system error that, for fifty percent (50%) or more of Participating Agency's users, substantially impairs use of one or more features or functions of the system.

- **“Severity level 3 error”** means any system error that, for fifty percent (50%) or more of Participating Agency’s users, has a minimal impact on the performance or operation of the system.

EXHIBIT [B]: PAYMENTS AND RATES

Peregrine Services
Effective Date: January 31, 2026
Initial Term: From the Effective Date through July 31, 2027("Initial Term").
Service Fee: The following fee schedule is available to the County of San Mateo ("County") if Order Form is signed on or before January 31, 2026. Unless otherwise terminated as set forth in the Terms and Conditions, County shall pay Peregrine a service fee of $1,414,500 annually for the Term as follows: a. **Initial Term (January 31, 2026 through January 30, 2027):** $1,414,500 within 30 days of the Effective Date The County has the option to continue use of the Service for up to two (2) optional annual terms as follows: b. **Option Year 1 (January 31, 2027 through January 30, 2028):** $971,290 within 30 days of January 31, 2027 c. **Option Year 2 (January 31, 2028 through January 30, 2029):** $1,000,428 within 30 days of January 31, 2028 The Participating Agency pricing set forth below reflects annualized twelve (12)-month reference pricing and is provided solely to illustrate the allocation of the eighteen (18)-month Initial Term Service Fee across Participating Agencies. The total Service Fee for the Initial Term is $1,414,500, which represents eighteen (18) months of Services and governs the County's payment obligation. The Participating Agency pricing does not represent separate or additive fees and is not intended to reflect eighteen (18)-month pricing at the agency level. Participating Agency Annualized Reference Pricing (12-Month Basis) for the Initial Term: San Mateo Police Department: $94,600 South San Francisco Police Department: $64,400 Daly City Police Department: $91,6330 San Bruno Police Department: $43,600 Pacifica Police Department: $36,800 Redwood City Police Department: $72,100 Hillsborough Police Department: $33,700 Foster City Police Department: $38,900 Menlo Park Police Department: $42,100 Atherton Police Department: $30,300 Burlingame Police Department: $38,900 Belmont Police Department: $34,600 East Palo Alto Police Department: $37,200 Colma Police Department: $28,400

San Mateo County Sheriff's Office: $160,700

San Mateo County District Attorney's Office: $32,000

Brisbane Police Department: $28,800

Broadmoor Police Department: $26,100

The pricing set forth in this Exhibit B reflects the annualized pricing applicable to each Participating Agency identified herein for the Initial Term. After the Initial Term, prices shall escalate at a rate of 3% annually. Such pricing shall apply regardless of whether Participating Agencies continue collectively or individually and shall not be impacted by any Participating Agency's decision to opt out following the Initial Term. During the Initial Term, the County shall administer payment on behalf of itself and the Participating Agencies.

Additional Data Source Pricing

In addition to the data source integrations described in Exhibit A (Services), Participating Agencies may purchase additional data source integrations during the Term.

Pricing for any such additional data source integration shall not exceed Thirty-Five Thousand Dollars ($35,000) per data source.

Any additional data source integrations purchased pursuant to this Section shall be subject to the same pricing structure and payment administration provisions set forth in this Exhibit B.

Users: The County may allow an unlimited number of employees of the Participating Agencies as identified in Exhibit A to access and use the Service during the applicable contract term; provided that, if a Participating Agency elects to opt out, employees of that Participating Agency shall no longer be authorized to access or use the Service.

Onboarding and Training Services: Peregrine will provide the County with an introductory training session that provides an overview of the Service, background on accessible data sources as of the Effective Date and an introduction to the analytic capabilities of the Service. Training is delivered during implementation through cross-functional workshops, periodic table-top exercises, and role-based sessions tailored to user needs. Upon kickoff, Peregrine will work with the County to determine the appropriate training approach and format.

Peregrine will provide additional training, including refresher sessions and advanced training modules, from time to time upon mutual agreement of the parties. Training may be conducted virtually or in person, as agreed. Ongoing training is available upon request and through self-help resources. The County will not be charged for training or trainer travel related to initial onboarding and training.

Professional Services: The initial County Data sources and systems that Peregrine will integrate with the Service for the County are listed in Exhibit A.

The County is responsible for any third-party API or data access fees.

Any additional data integrations or new functionality shall be subject to mutual written agreement of the parties, including with respect to fees. All additional data integration services or new functionality and corresponding fees will be set forth in a statement of work.

Peregrine_20270731

Final Audit Report 2026-01-22

Created:	2026-01-22
By:	Veronica Ruiz (vruiz@smcgov.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAvhkOKy_3OL7vyGdqF724P9Ex9YeeNc8k

"Peregrine_20270731" History

Document created by Veronica Ruiz (vruiz@smcgov.org)
2026-01-22 - 5:13:55 PM GMT- IP address: 136.226.78.111

Document emailed to rob.wheeler@peregrine.io for signature
2026-01-22 - 5:17:45 PM GMT

Email viewed by rob.wheeler@peregrine.io
2026-01-22 - 5:18:22 PM GMT- IP address: 104.47.64.254

rob.wheeler@peregrine.io authenticated with Adobe Acrobat Sign.
2026-01-22 - 5:21:59 PM GMT

Signer rob.wheeler@peregrine.io entered name at signing as William R Wheeler
2026-01-22 - 5:22:29 PM GMT- IP address: 24.118.51.188

Document e-signed by William R Wheeler (rob.wheeler@peregrine.io)
Signature Date: 2026-01-22 - 5:22:31 PM GMT - Time Source: server- IP address: 24.118.51.188

Agreement completed.
2026-01-22 - 5:22:31 PM GMT