Madera County Cloud Services Addendum

This Cloud Computing Services Addendum ("Addendum"), is by and between _____ ("Vendor"), and MADERA COUNTY ("County"). Vendor and County agree that the following terms and conditions will apply to the services provided under the Agreement this Addendum is incorporated therein. The parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for the parties to comply with the requirements of all applicable federal and California statutes and regulations governing confidentiality and privacy.

1. DEFINITIONS - Whenever used in this Addendum, the following terms shall have the meanings assigned below. Other capitalized terms used in this Addendum are defined in the context in which they are used or as defined in accompanying contract documents.

1.1 "**Agreement**" means the document provided by the Vendor that contains terms of service, use, and work that will take place between the parties in return for consideration.

1.2 "**Confidential Data**" means any Data that a disclosing party treats in a confidential manner or that is marked "Confidential" prior to disclosure to the other party. Confidential Data does not include information which: (a) is public or becomes public through no breach of the confidentiality obligations herein; (b) is disclosed by the party that has received the data (the "Receiving Party") with the prior written approval of the other party; (c) was known by the Receiving Party at the time of disclosure; (d) was developed independently by the Receiving Party without use of confidential Information; (e) becomes known to the Receiving Party from a source other than the disclosing party through lawful means; (f) is disclosed by the disclosing party to others without confidentiality obligations; or (g) is required by law to be disclosed.

1.3 "**County Data**" means Data created or caused to be created by the County and includes credentials issued to County by Vendor and all records relating to County's use of Vendor Services and administration of End User accounts, including any Protected Information of County personnel that does not otherwise constitute Protected Information of an End User.

1.4 "**Cover Sheet**" means the document provided by the County that incorporates all documentation, including by not limited, to the Vendor's Agreement and Exhibits, which comprises the complete terms of the final contract that will exist between the parties.

1.5 "**Data**" means all information, whether in oral or written (including electronic) form, created by or in any way originating with County and End Users, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or in any way originating with County and End Users, in the course of using and configuring the Services provided under this Agreement, and includes County Data, End User Data, and Protected Information.

1.6 "**Data Compromise**" means any actual or reasonably suspected unauthorized access to or acquisition of computerized Data that compromises the security, confidentiality, or integrity of the Data, or the ability of County to access the Data. Data Compromise also means a "Breach" as defined under relevant California or federal law for Protected Information, for example, California Civil Code Section 1798.29, California Health and Safety Code Section 1280.15, etc.

1.7 "**Documentation**" means, collectively: (a) all materials published or otherwise made available to County by Vendor that relate to the functional, operational and/or performance capabilities of the Services; (b) all user, operator, system administration, technical, support and other manuals, diagrams, topology, and all other materials published or otherwise made available by Vendor that

describe the functional, operational and/or performance capabilities of the Services; (c) any Requests for Information and/or Requests for Proposals (or documents of similar effect) issued by County, and the responses thereto from Vendor, and any document which purports to update or revise any of the foregoing; and (d) the results of any Vendor presentations or tests provided by Vendor to County.

1.8 "**Downtime**" means any period of time of any duration that the Services are not made available by Vendor to County for any reason, including scheduled maintenance or Enhancements.

1.9 "**End User**" means the individuals authorized by County to access and use the Services provided by Vendor under this Agreement including, but not limited to, employees, authorized agents, extra help, and volunteers of County; Third Party consultants, auditors and other independent Vendors performing services for County; any governmental, accrediting or regulatory bodies lawfully requesting or requiring access to any Services; customers of County provided services; and any external users collaborating with County.

1.10 "**End User Data**" means Data created by an End User and includes, but is not limited to, End User account credentials and information, and all records sent, received, or created by or for End Users, including email content, headers, and attachments, and any Protected Information of any End User or Third Party contained therein or in any logs or other records of Vendor reflecting End User's use of Vendor Services.

1.11 "**Enhancements**" means any improvements, modifications, upgrades, updates, fixes, revisions and/or expansions to the Services that Vendor may develop or acquire and incorporate into its standard version of the Services or which the Vendor has elected to make generally available to its customers.

1.12 "**Force Majeure**" means an event such as an act of God; fire, flood; storm; inclement weather; earthquake; drought; riot; war or insurrection; plant or animal infestation or disease; sudden or severe energy shortage; or other condition of emergency or disaster beyond the control of the Parties which makes performance of obligations under this Agreement impossible or extremely impracticable, such obligations shall be suspended during such time any such condition or conditions exist. If a party's duties are suspended, that party shall resume its obligation at the earliest practical time.

1.13 "**Project Manager**" means the individual who shall serve as each party's point of contact with the other party's personnel as provided in this Agreement. The initial Project Managers and their contact information are set forth in the Notices section below and may be changed by a party at any time upon written notice to the other party.

1.14 "**Protected Information**" means Data connected to the identify of individuals and includes but is not limited to personally-identifiable information (PII), employee records, protected health information (PHI), Criminal Justice Information (CJI), Federal Tax Information (FTI) protected under Publication 1075, Social Security Administration (SSA), or individual financial information that is subject to state or federal laws restricting the use and disclosure of such information, including, but not limited to, Article 1, Section 1 of the California Constitution; the California Information Practices Act (Civil Code § 1798 et seq.); the California Confidentiality of Medical Information Act (Civil Code § 56 et seq.); the federal Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801 through 6809; and the privacy and information security aspects of the Administrative Simplification provisions of the federal Health Insurance Portability and Accountability Act (45 CFR Part 160 and Subparts A, C, and E of Part 164).

1.15 "**Services**" means Vendor's computing solutions, provided over the Internet to County pursuant to this Agreement, that provide the functionality and/or produce the results described in the Documentation, including without limitation all Enhancements thereto and all interfaces.

1.16 "**Third Party**" means persons, corporations and entities other than Vendor, County or any of their employees, Vendors or agents.

2. SCOPE OF ADDENDUM

2.1 The Services included under this Addendum are as determined in the Agreement or Cover Sheet, which this Addendum is attached and incorporated by reference therein.
2.2 All Services provided by Vendor that are provided online shall be Web Content Accessibility Guidelines (WCAG) 2.0 AA compliant.

3. RIGHTS AND LICENSE IN AND TO COUNTY AND END USER DATA

3.1 The parties agree that as between them, all rights including all intellectual property rights in and to data and information provided by County or on behalf of County or created by Vendor in the performance of services hereunder shall remain the exclusive property of County. Vendor has a limited, nonexclusive license to use End User Data and County Data and other information solely for the purpose of performing its obligations under this Agreement. This Agreement does not give Vendor any rights, implied or otherwise, data, information, or intellectual property, except as expressly stated in this Agreement.
3.2 County retains the right to use the Services to access and retrieve County and End User Data stored on Vendor's Services infrastructure at any time at its sole discretion.
3.3 Vendor will provide data retrieval to the County within 72 hours of official request. Data will be provided in a universal format such as comma separated values (.CSV).

4. DATA PRIVACY

4.1 Vendor will use County Data and End User Data only for the purpose of fulfilling its duties under this Agreement and for County's and its End User's sole benefit, and will not share such Data with or disclose it to any Third Party without the prior written consent of County or as otherwise required by law. By way of illustration and not of limitation, Vendor will not use such Data for Vendor's own benefit and, in particular, will not engage in "data mining" of County or End User Data or communications, whether through automated or human means, except as specifically and expressly required by law or authorized in writing by County.
4.2 All Data will be stored on servers located solely within the Continental United States.
4.3 Vendor will provide access to County and End User Data only to those Vendor employees, Vendors and subcontractors ("Vendor Staff") who need to access the Data to fulfill Vendor's obligations under this Agreement. Vendor will ensure that, prior to being granted access to the Data, Vendor Staff who perform work under this Agreement have all undergone and passed criminal background screenings; have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all Data protection provisions of this Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the Data they will be handling.

5. DATA SECURITY AND INTEGRITY

5.1 All facilities used to store and process County and End User Data will implement and maintain administrative, physical, technical, and procedural safeguards and best practices at a level sufficient to secure such Data in accordance of the American Institute of CPAs (AICPA)'s Service Organization Control (SOC) reporting platform SOC II compliance requirements. Vendor will provide proof of a current SOC II Compliance certification.

5.2 Prior to the Effective Date of this Agreement, Vendor will at its expense conduct or have conducted the following, and thereafter, Vendor will at its expense conduct or have conducted the following at least once per year, and immediately after any actual or reasonably suspected Data Compromise:

5.2.1 A SSAE 18/SOC 2 audit of Vendor's security policies, procedures and controls.

5.2.2 Certification under "NIST FIPS 200 AND SP 800-53", "ISO 27001/27002", or other acceptable standard cloud computing services certification.

5.2.3 A vulnerability scan, performed by a County-approved Third Party scanner, of Vendor's systems and facilities that are used in any way to deliver Services under this Agreement.

5.2.4 A formal penetration test, performed by a process and qualified personnel approved by County, of Vendor's systems and facilities that are used in any way to deliver Services under this Agreement.

5.3 Vendor will provide County the reports or other documentation resulting from the above audits, certifications, scans and tests within seven (7) business days of Vendor's receipt of such results.

5.4 Based on the results of the above audits, certifications, scans and tests, Vendor will, within thirty (30) calendar days of receipt of such results, promptly modify its security measures in order to meet its obligations under this Agreement, and provide County with written evidence of remediation.

5.4.1 County may require, at no expense to the County, that Vendor perform additional audits and tests, the results of which will be provided to County within seven (7) business days of Vendor's receipt of such results should the results of the annual audit not meet the terms of this Addendum.

5.5 Vendor shall protect County and End User Data against deterioration or degradation of Data quality and authenticity, including, but not limited to annual Third Party Data integrity audits. Vendor will provide County the results of the above audits, along with Vendor's plan for addressing or resolving any shortcomings identified by such audits, within seven (7) business days of Vendor's receipt of such results.

5.6 Vendor will provide County with Service Redundancy to ensure system availability in the event of natural disaster or unanticipated system outages. Redundancy shall include the following four (4) areas:

5.6.1 Hardware Redundancy

5.6.2 Processing Redundancy

5.6.3 Geographic Redundancy

5.6.4 Network Redundancy

5.7 Without limiting the foregoing, Vendor warrants that all County Data and End User Data will be encrypted in transmission (including via web interface) and in storage at a level equivalent to or stronger than 128-bit level encryption using a FIPS 140-2 certified algorithm such as AES or TLS. It is encouraged, when available and when feasible, that 256 bit encryption is used.

5.7.1 This requirement pertains to any type of sensitive data in motion such as website access, file transfer, and email.

5.7.2 Servers which use, store, use and/or process, also known as data at rest, Confidential Data shall be encrypted using FIPS 140-2 certified algorithm 128 bit or higher, such as Advanced Encryption (AES). The encryption solution must be full disk. It is encouraged, when available and when feasible, that the encryption be at 256 bit.

5.8 Vendor shall at all times ensure security vulnerabilities (hardware, software, and firmware) are appropriately patched within seven (7) days of vendor release. Critical security patches released by vendors shall be patched by the Vendor within forty-eight (48) hours of vendor release. Patches shall be adequately tested prior to installation. If system interruption is anticipated for patch installation, County shall be notified with a minimum of forty-eight (48) hour notice.

5.9 Vendor shall at all times use industry-standard and up-to-date security tools, technologies and procedures including, but not limited to anti-virus and anti-malware protections and intrusion detection and reporting methods.

5.10 Vendor will configure the Services to filter spam while permitting communications from Third Party Internet Protocol addresses identified by County as legitimate.

5.11 Vendor will include a schedule of patches and software releases with a written report to County regarding patch installation.

5.12 Vendor will ensure multi-factor authentication of Protected Information is available when County is required to provide such authentication for regulatory compliance.

6. DATA COMPROMISE RESPONSE

6.1 Vendor shall report, either orally or in writing, to County any Data Compromise involving County or End User Data, or circumstances that could have resulted in unauthorized access to or disclosure or use of County or End User Data, not authorized by this Agreement or in writing by County, including any reasonable belief that an unauthorized individual has accessed County or End User Data. Vendor shall make the report to County immediately upon discovery of the unauthorized disclosure, but in no event more than forty-eight (48) hours after Vendor reasonably believes there has been such unauthorized use or disclosure. Oral reports by Vendor regarding Data Compromises will be reduced to writing and supplied to County as soon as reasonably practicable, but in no event more than forty-eight (48) hours after oral report.

6.2 Immediately upon becoming aware of any such Data Compromise, Vendor shall fully investigate the circumstances, extent and causes of the Data Compromise, and report the results to County and continue to keep County informed on a daily basis of the progress of its investigation until the issue has been effectively resolved.

6.3 Vendor's report discussed herein shall identify: (i) the nature of the unauthorized use or disclosure, (ii) the County or End User Data used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure (if known), (iv) what Vendor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action Vendor has taken or shall take to prevent future similar unauthorized use or disclosure.

6.4 Within five (5) calendar days of the date Vendor becomes aware of any such Data Compromise, Vendor shall have completed implementation of corrective actions to remedy the Data Compromise, restore County access to the Services as directed by County, and prevent further similar unauthorized use or disclosure.

6.5 Vendor, at its expense, shall cooperate fully with County's investigation of and response to any such Data Compromise incident.

6.6 Except as otherwise required by law, Vendor will not provide notice of the incident directly to the persons whose Data were involved, regulatory agencies, or other entities, without prior written permission from County.

6.7 Notwithstanding any other provision of this agreement, and in addition to any other remedies available to County under law or equity, Vendor will promptly reimburse County in full for all costs incurred by County in any investigation, remediation or litigation resulting from any such Data Compromise, including but not limited to providing notification to Third Parties whose Data were compromised and to regulatory bodies, law enforcement agencies or other entities as required by law or contract; establishing and monitoring call center(s), and credit monitoring and/or identity restoration services to assist each person impacted by a Data Compromise in such a fashion that, in County's sole discretion, could lead to identity theft; and the payment of legal fees and expenses, audit costs, fines and penalties, and other fees imposed by regulatory agencies, courts of law, or contracting partners as a result of the Data Compromise.

7. AUDIT TRAIL

7.1 Vendor will retain logs associated with End User activity for the length of time communicated to the Vendor by the County in the Cover Sheet, or, if no length of time is communicated, logs shall be maintained for a minimum of three (3) years.

7.1.1 The systems which provided to County by Vendor shall maintain an automated audit trail that can identify the user or system process which initiates a request for Confidential Data.

7.1.2 The audit trail shall:

7.1.2.1 Be date and time stamped;

7.1.2.2 Log both successful and failed accesses;

7.1.2.3 Be read-only; and

7.1.2.4 Be restricted to authorized users.

7.1.3 Audit log information shall be provided to the County, or other authorized personnel approved by the County, upon written request within seventy-two (72) hours.

7.1.4 If Confidential Data is stored in the database logging functionality shall be enabled.

7.1.5 Audit trail data shall be archived for, the length of time as communicated Vendor by the County in the Cover Sheet, if no amount is communicated, data shall be archived for at least three (3) years from the occurrence or as otherwise required by federal or State law.

8. DATA RETENTION AND DISPOSAL

8.1 Vendor shall retain End User Data, including attachments, until the End User deletes them or for at least seven (7) years from the last time the End User account was accessed or as otherwise required by federal or state law.

8.2 Vendor shall document data backup policies; upon request of the County, shall provide proof of data backup policies.

8.3 Using appropriate and reliable storage media, Vendor will regularly backup County and End User Data and retain such backup copies for a minimum of twelve (12) months.

8.4 Vendor shall document data retention policies; upon request of the County, shall provide proof of data retention policies.

8.5 At the County's election, Vendor will either securely destroy or transmit to County repository any backup copies of County and/or End User Data. Vendor will supply County a certificate indicating the records disposed of, the date disposed of, and the method of disposition used. Data destruction shall be disposed of through confidential means, such as cross cut shredding or pulverizing based on National Institute of Standards and Technology (NIST) SP 800-88.

8.6 Vendor will immediately place a "hold" on Data destruction or disposal under its usual records retention policies of records that include County's and End User Data, in response to an oral or written request from County indicating that those records may be relevant to litigation that County reasonably anticipates. Oral requests by County for a hold on record destruction will be reduced to writing and supplied to Vendor for its records as soon as reasonably practicable under the circumstances. County will promptly coordinate with Vendor regarding the preservation and disposition of these records. Vendor shall continue to preserve the records until further notice by County.

9. DATA TRANSFER UPON TERMINATION OR EXPIRATION

9.1 Upon termination or expiration of this Agreement, Vendor will ensure that all County and End User Data are securely transferred to County, or a Third Party designated by County, within fourteen (14) calendar days, all as further specified in the technical specifications provided in official request to Vendor. Vendor will ensure that such migration uses facilities and methods that are compatible with the relevant systems of County, and that County will have access to County and End User Data during the transition. In the event that it is not possible to transfer the aforementioned data to County in a format that does not require proprietary software to access the data, Vendor shall provide County with an unlimited use, perpetual license to any proprietary software necessary in order to gain access to the data.

9.2 Vendor will provide County with no less than ninety (90) calendar days-notice of impending cessation of its business or that of any Vendor subcontractor and any contingency plans in the event of notice of such cessation. This includes immediate transfer of any previously escrowed assets and Data and providing County access to Vendor's facilities to remove and destroy County-owned assets and Data.

9.3 Along with the notice described above, Vendor will provide a fully documented service description and perform and document a gap analysis by examining any differences between its Services and those to be provided by its successor.

9.4 Vendor will provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to County.

9.5 Vendor shall implement its contingency and/or exit plans and take all necessary actions to provide for an effective and efficient transition of service with minimal disruption to County. Vendor will work closely with its successor to ensure a successful transition to the new service and/or equipment, with minimal Downtime and effect on County, all such work to be coordinated and performed no less than ninety (90) calendar days in advance of the formal, final transition date.

10. SERVICE LEVELS

10.1 Services levels shall be provided in the manner and to the standards are referenced in the Agreement. In the event the Agreement does not include service levels, Vendor shall provide services to the County as in County's Service Level Agreement which will be attached hereto as **Exhibit A.**

11. INTERRUPTIONS IN SERVICE; SUSPENSION AND TERMINATION OF SERVICE; CHANGES TO SERVICE

11.1 Notwithstanding the Force Majeure provisions contained herein, Vendor shall be responsible for providing disaster recovery Services if Vendor experiences or suffers a disaster. Vendor shall take all necessary steps to ensure that County shall not be denied access to the Services for more than five (5) hours in the event there is a disaster impacting any Vendor infrastructure necessary to provide the Services. Vendor shall maintain the capability to resume provisions of the Services from an alternative location and via an alternative telecommunications route in the event of a disaster that renders the Vendor's primary infrastructure unusable or unavailable. If Vendor fails to restore the Services within five (5) hours of the initial disruption of service, County may declare Vendor to be in default of this Agreement and County may seek alternate services, which would have otherwise been provided under this Agreement, from Third Parties. Vendor shall reimburse County for all costs reasonably incurred by County in obtaining such alternative services, with payment to be made within thirty (30) calendar days of County's written request for such payment.

11.2 In the event of a service outage, Vendor will refund or credit County, at County's election, the pro-rated amount of fees corresponding to the time Services were unavailable.

11.3 Vendor warrants that the minimum technical requirements for access to and operation of the Services are FIREFOX (Latest Stable Version), CHROME (Latest Stable Version), MICROSOFT EDGE (Latest Stable Version). Mobile browser by Firefox and Chrome. If future Enhancements to the Services require use of newer versions of these web browsers, Vendor will provide a minimum hundred and eighty (180) days written notice to County prior to implementing such Enhancements. Any browser plug-in's (e.g. Java, ActiveX, etc.) required by Vendor for Service functionality shall be discussed with County and mutually agreed upon. Any changes to such plug-in's resulting in changes to Service functionality shall be provided to County by written notice hundred and eighty (180) days prior to implementing Enhancements.

11.4 From time to time it may be necessary or desirable for either the County or Vendor to propose changes in the Services provided. Such changes shall be submitted to the other Party in writing for review and acceptance. Automatic Enhancements to any software used by Vendor to provide the Services that simply improve the speed, efficiency, reliability, or availability of existing Services and do not alter or add functionality, are not considered "changes to the Services" and such Enhancements will be implemented by Vendor on a schedule no less favorable than provided by Vendor to any other customer receiving comparable levels of Services.

11.5 Vendor will provide County with thirty (30) calendar days prior notice of any times that the Services will be unavailable due to non-emergency maintenance or Enhancements. Vendor will schedule any such times that the Services will be unavailable during non-business hours preferably between the hours of 12:00AM – 4:00AM PST. In the event of unscheduled and unforeseen times that the Services will for any reason, except as otherwise prohibited by law, Vendor will immediately notify County and cooperate with County's reasonable requests for information regarding the Services being unavailable (including causes, effect on Services, and estimated duration).

11.6 County may suspend or terminate (or direct Vendor to suspend or terminate) an End User's access to Services in accordance with County's policies. County will assume sole responsibility for any claims made by End User regarding County's suspension/termination or directive to suspend/terminate such Services.

11.7 Vendor may suspend access to Services by an End User immediately in response to an act or omission that reasonably appears to jeopardize the security or integrity of Vendor's Services or the network(s) or facilities used to provide the Services. Suspension will be to the minimum extent, and of the minimum duration, required to prevent or end the security issue. The suspension will be lifted immediately once the breach is cured. Vendor may suspend access to Services by an End User in response to a material breach by End User of any terms of use s/he has agreed to in connection with receiving the Services. Vendor will immediately notify County of any suspension of End User access to Services.

11.8 Vendor may suspend access to Services by County in response to an act or omission that poses a significant threat to the security or integrity of Vendor's Services or the network(s) or facilities used to provide the Services. Vendor will provide County with at least fifteen (15) business days advance written notice of intent to suspend and justification for suspension. County will have fifteen (15) business days to review and respond to such notice, and to correct any such action or omission prior to suspension. If County's response resolves the issue to the parties' mutual satisfaction, suspension will not occur. If County is unable to resolve the issue within the stated timeframe, then suspension will be to the minimum extent, and of the minimum duration, required to prevent or end the security issue. Any such suspension will be lifted immediately once the breach is cured.

12. TECHNICAL SUPPORT

12.1 Technical shall be provided in the manner and to the standards are referenced in the Agreement. In the event the Agreement does not include technical support, Vendor shall provide services to the County as in County's Maintenance Agreement which will be attached hereto as **Exhibit B.**

13. TRANSITION ASSISTANCE

13.1 Vendor will develop, provide and implement the following transition assistance ("Transition Assistance") to support County's successful and uninterrupted transition from its current solution, or other solution in this area, to Vendor's Services. Transition Assistance will be provided by Vendor as detailed below at no additional cost to County. Transition assistance will be provided by Vendor at County at mutually agreeable dates and times, but no later than ten (10) calendar days following the Effective Date of this Agreement.

13.2 Within no more than ten (10) calendar days after the Effective Date of this Agreement, Vendor shall, at its own expense, provide qualified individuals to (a) uninstall existing solution, (b) implement the Services, and (c) assist in testing of the Services to ensure that they are functioning in accordance with the terms of this Agreement.

13.3 Vendor's Project Manager shall coordinate with County's Project Manager, and they shall develop a mutually agreeable installation plan and schedule for the assistance provided above.

13.4 If and when applicable, the installation plan shall provide for:

13.4.1 The timely and successful integration of Vendor software, applications and Services with County's existing identity management and access management systems Cisco ISE and Microsoft Active Directory.

13.4.2 The timely and successful integration with specified County applications as mutually agreed upon by Vendor and provided in writing by the County.

13.4.3 The availability of and support for the Services via specified County and End User devices including mobile devices; and

13.4.4 County's ability to, directly or through instructions to Vendor, create, modify, suspend, eliminate, assign aliases for, and internally delegate the administration of, individual and group accounts created as part of Vendor's provision of Services.

13.5 County agrees (a) to have the site(s) at which the Services will be used prepared in accordance with applicable Vendor requirements prior to the Effective Date of the installation plan and schedule; and (b) maintain the site(s) at its own expense subsequent to completion of the installation plan and schedule. County shall provide any and all necessary utility services for use of the Services.

13.6 In connection with Vendor's Transition Assistance, County will provide information, Data, computer access and time, work space, forms, data entry and telephone service and personnel reasonably necessary to assist Vendor consistent with County's policies and procedures.

13.7 In the event that Vendor fails to meet the target date for completion of transition, Vendor shall credit County ten percent (10%) of the monthly Services fees for every business day the transition is late. If Vendor misses the target date by more than thirty (30) calendar days, Vendor shall be in breach of the Agreement.

14. PROTECTED INFORMATION

14.1 In connection with the use of the Services provided by Vendor hereunder, County may disclose to Vendor Protected Information. Vendor agrees to protect the privacy and security of Protected Information. Vendor shall be beholden to all applicable sections of Madera County Contracts between the State of California and Madera County pertaining to security measures and breach protocol protecting Protected Information as identified in [name of document(s)] and is/are attached herein [collectively] as **Exhibit C.**

14.1.1 Vendor shall implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of the Protected Information. Vendor shall have documented countermeasures to protect physical assets in the event of a disaster. Documentation will be provided to the County upon request. At the request of the County, Vendor will be required to perform a 3rd party physical audit by a Vendor of the County's choice, at no additional cost to the County. All Protected Information stored on portable devices or media must be encrypted in accordance with the Federal Information Processing Standards (FIPS) Publication 140-2. Vendor shall ensure that such security measures are regularly reviewed and revised to address evolving threats and vulnerabilities while Vendor has responsibility for the Protected Information under the terms of this Addendum. Prior to execution of the Agreement, and periodically thereafter (no more frequently than annually) at the County's request, Vendor will provide assurance, in the form of a third-party audit report or other documentation acceptable to the County.

14.2 Vendor agrees to hold the County's Protected Information, and any information derived from such information, in strictest confidence. Vendor shall not access, use or disclose Protected Information

except as permitted or required by the Agreement or as otherwise authorized in writing by County, or applicable laws. If required by a court of competent jurisdiction or an administrative body to disclose Protected Information, Vendor will notify County in writing immediately upon receiving notice of such requirement and prior to any such disclosure, to give County an opportunity to oppose or otherwise respond to such disclosure (unless prohibited by law from doing so). Any transmission, transportation or storage of Protected Information outside the United States is prohibited except on prior written authorization by the County.

14.3 Within 30 days of the termination, cancellation, expiration or other conclusion of the Agreement, Vendor shall return the Protected Information to County unless County requests in writing that such data be destroyed. This provision shall also apply to all Protected Information that is in the possession of subcontractors or agents of Vendor. Such destruction shall be accomplished by "purging" or "physical destruction," in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-88. Vendor shall certify in writing to County that such return or destruction has been completed.

14.4 Costs. In the event of Data Compromise, Vendor agrees to promptly reimburse all costs to the County arising from such Data Compromise pursuant to federal and/or State law, including but not limited to costs of notification of individuals, establishing and operating call center(s), credit monitoring and/or identity restoration services, time of County personnel responding to Breach, civil or criminal penalties levied against the County, attorneys fees, court costs, etc. Any Data Compromise may be grounds for immediate termination of this Agreement by the County.

15. ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS

15.1 Vendor shall make itself and any employees, subcontractors, or agents assisting Vendor in the performance of its obligations under the Agreement available to County at no cost to County to testify as witnesses, or otherwise, in the event of an unauthorized disclosure caused by Vendor that results in litigation or administrative proceedings against County, its directors, officers, agents or employees based upon a claimed violation of laws relating to security and privacy and arising out of this Addendum.

16. SURVIVAL

16.1 The terms and conditions set forth in this Addendum shall survive termination of the Agreement between the parties. If Vendor is unable to return or destroy the County's Protected Information in accordance with Article 6, then this Addendum, in its entirety, shall survive the Agreement until such time as Vendor does return or destroy the Protected Information.

17. SUBCONTRACTOR

17.1 Vendor agrees to include all of the terms and conditions contained in this Addendum in all subcontractor or agency contracts providing services under this Agreement.