DATA SHARING
MEMORANDUM OF UNDERSTANDING

This Memorandum of Understanding (hereinafter "MOU" or "Agreement") is made and entered into this __ day of _____, 2025 by and between the County of San Mateo, on behalf of the San Mateo County Sheriff's Office ("SMCSO") and the following entities:

- the Town of Atherton, a California municipal corporation on behalf of the Atherton Police Department ("Atherton"),
- the City of Belmont, a California municipal corporation on behalf of the Belmont Police Department ("Belmont"),
- the City of Brisbane, a California municipal corporation on behalf of the Brisbane Police Department ("Brisbane"),
- the Town of Broadmoor a California municipal corporation on behalf of the Broadmoor Police Department, ("Broadmoor"),
- the City of Burlingame a California municipal corporation on behalf of the Burlingame Police Department, ("Burlingame"),
- the City of Colma, a California municipal corporation on behalf of the Colma Police Department ("Colma")
- the City of Daly City, a California municipal corporation on behalf of the Colma Police Department ("Daly City"),
- the City of East Palo Alto, a California municipal corporation on behalf of the East Palo Alto Police Department ("East Palo Alto"),
- the City of Foster City, a California municipal corporation on behalf of the Foster City Police Department ("Foster City"),
- the City of Menlo Park, a California municipal corporation on behalf of the Menlo Park Police Department ("Menlo Park"),
- the City of Pacifica, a California municipal corporation on behalf of the City of Pacifica Police Department ("Pacifica"),
- the City of Redwood City, a California municipal corporation on behalf of the Redwood City Police Department ("Redwood City"),
- the City of San Bruno, A California municipal corporation on behalf of the San Bruno Department ("San Bruno"),
- the City of San Mateo, a California municipal corporation on behalf of the San Mateo Police Department ("San Mateo"),
- and the City of South San Francisco, a California municipal corporation on behalf of the South San Francisco Police Department ("South San Francisco").

SMCSO, Atherton, Belmont, Brisbane, Broadmoor, Burlingame, Colma, Daly City, East Palo Alto, Foster City, Menlo Park, Pacifica, Redwood City, San Bruno, San Mateo, and South San Francisco may collectively be referred to as "Parties" and individually referred to as "Party."

RECITALS

WHEREAS, the Parties provide public safety services within their jurisdictions; and

WHEREAS, the Parties have found it to be of mutual benefit to provide for the most efficient utilization of their resources and services in the application to public safety efforts within their jurisdictions; and

WHEREAS, the Parties are committed to cooperation and coordination in providing the highest level of safety services to the public, guided by the principle that cooperative efforts are in the public's best interest; and

WHEREAS, the Parties support the sharing of information contained within their respective electronic data systems in furtherance of collaboration with other Criminal Justice Information Services ("CJIS") Compliant public safety entities, through integrated systems of information technology that the Parties have developed, established, and/or licensed; and

WHEREAS, the Parties intend that confidential records or information shared between the Parties under this Agreement will be subject to Government Code Section 7921.505(c)(5), which protects from disclosure under the California Public Records Act exempt or privileged records that one governmental agency shares with another governmental agency pursuant to an agreement that the latter will treat the disclosed records as confidential; and

WHEREAS, the Parties agree that every Party receiving confidential records or information under this Agreement will treat the disclosed records as confidential; and

WHEREAS, the Parties recognize the need to protect each Party's ownership and control over its shared information, to optimize the means through which shared information is accessed or analyzed, and to protect privacy and civil liberties in accordance with the law; and

WHEREAS, the Parties further desire to share information contained within their electronic data systems under the conditions set forth in this MOU.

NOW, THEREFORE, for and in consideration of the covenants contained herein, the Parties hereby agree as follows:

AGREEMENT

I. PURPOSE

The purpose of this MOU is to provide a standardized approach and method of collection and sharing of information within the respective electronic data systems between the Parties and to facilitate bi-directional data collaboration among other CJIS Compliant public safety agencies in a manner that is consistent with the Parties' obligations, rights and applicable laws and regulations, including the California Values Act.

II. DEFINITIONS AND OTHER TERMINOLOGY

Authorized Users: Personnel (employees and/or independent contracts) of a Party that have the appropriate clearance and authority to utilize and access shared data as a function of their employment, in support of law enforcement or public safety investigatory activity.

Data: Electronic records, analyses, images, and other information associated with incidents, persons, or objects, originally created by a Party and existing in a Party's system or database.

Contributed Data: Records originating from a Party that a Party has elected to share with other appropriate parties.

C3 AI Law Enforcement System: An integrated, artificial intelligence ("AI")-powered intelligence analysis software solution that enhances public safety by efficiently integrating disparate data sources into a single, searchable platform for law enforcement personnel to derive investigative insights in near real-time.

Data Repository: An enterprise data storage entity or entities into which data has been specifically partitioned for an analytical or reporting purpose.

Shared Data: The aggregate pool of shared information from Member Agencies and other contributing sources, made available via SMCSO or facilitated by SMCSO-hosted technology systems, and/or efforts.

III. DATA ACCESS

A. Data contributed by each Party will be shared with all Parties that have entered into this MOU. The Parties agree not to facilitate information sharing between law enforcement entities that have not entered into agreements allowing such sharing.

B. Nothing in this Agreement shall be construed to require a Party:

1. To disclose information owned and controlled by a Party, if the Party determines, in its sole discretion, it does not have the ability or authority to disclose;

2. To perform any act that a Party determines, is contrary to law or public policy;

3. To provide personnel, equipment, or services to another Party; or

4. To modify data owned by another Party or inhibit or restrict any other Party or Parties use of its own information technology system or systems.

IV. DATA SHARING AND SECURITY

A. Requirements

Each Party has sole discretion to share the information it wishes to contribute and place restrictions on the recipient and/or audience to which contributed data may be shared. Parties are not required to contribute data to shared data repositories. In gathering, sharing, and storing information, and in all other respects in performing acts related to this Agreement, the Parties will comply with all applicable laws, rules, and regulations and agree to enforce and maintain security requirements for the information stored or shared in their respective data repositories, including but not limited to as specified in the California Values Act, the Information Practices Act, the Public Records Act, California Attorney General's Model Standards and Procedures for Maintaining Criminal Intelligence Files and Criminal Intelligence Operational Activities and 28 Code of Federal Regulations ("CFR") Part 23.

B. Security Standards

The Parties agree to enforce and maintain security for shared data in compliance with all applicable laws, including but not limited to the California Department of Justice's California Law Enforcement Telecommunications System Policies, Practices, and Procedures ("CLETS PPP"), the Federal Bureau of Investigation's Criminal Justice Information System Security Policy ("FBI CJIS Security Policy"), the California Attorney General's Model Standards and Procedures for Maintaining Criminal Intelligence Files and Criminal Intelligence Operational Activities and 28 CFR Part 23, Civil Code Section 1798.90.5 et seq, Government Code Section 34090.6, and each Party's Automated License Plate Reader ("ALPR") policy, if applicable.

The Parties shall store information, whether electronic or hardcopy, only in a manner that is compliant with all applicable physical security and cyber security requirements. Data shall be retained, purged, and destroyed in accordance with all applicable standards, inclusive of each Party's retention policy for their contributing data. Data exchange and user access shall be achieved using encryption, private networks, or other configurations that follow current best practices for information technology.

In compliance with the aforementioned CLETS PPP and FBI CJIS Security Policy, The Parties grant authority to SMCSO the duties and responsibilities of CLETS security clearances, which includes state and federal level fingerprint-based background checks of all C3 AI employees who have unescorted physical or logical access to CLETS-related hardware, software or unencrypted criminal justice information ("CJI") and maintenance of CLETS-related forms and records. Unless already known, Parties shall provide SMCSO the names of C3 AI employees who require unescorted physical or logical access to CLETS-related hardware, software or unencrypted CJI and request fingerprinting services prior to granting unescorted physical or logical access. SMCSO agrees to provide fingerprinting services within thirty (30) days of a request.

C. Approved Utilization

The Parties agree to use information residing in the shared data repositories, including but not limited to the C3 AI Law Enforcement platform, as a pointer system for investigative leads or guidance, and not as the sole source of probable cause for law enforcement actions. The Parties

further agree that the information hosted in the data repositories shall be used for law enforcement purposes only and that only law enforcement agency employees that have been subject to background screening will be allowed access to the system. Background screenings must be fingerprint based including checks of both the state and national criminal history repositories. If a felony conviction of any kind is found, access to the data repositories shall not be granted or otherwise revoked.

Consistent with the preceding paragraph, Parties acknowledge that data maintained in the C3 AI data repository system consists of information that may or may not be accurate. Parties neither warrant nor may they rely upon the accuracy of such information. Parties understand and agree to convey this caution to their employees who are Authorized Users. It shall be the responsibility of the Party or Authorized User requesting or using the data to confirm the accuracy of the information before taking any enforcement-related action.

D. Authorized Users

Each Party shall be responsible for training its users authorized to access information on the use and dissemination of information obtained from the C3 AI data repository system. Specifically, users must have a clear understanding of the need to verify the reliability of information with the source agency that contributed the information, when using information for purpose such as obtaining search and arrest warrants, affidavits, subpoenas, etc. Parties must also fully train and credential accessing users regarding the use of third-party information. Each Party is responsible for management of its Authorized User accounts and the activities of its Authorized Users.

E. Contribution of Data into C3 AI Law Enforcement System:

Each Party grants authority to SMCSO to provide contributed data into the C3 AI Law Enforcement system to optimize law enforcement sharing, search, reporting, or analytic capabilities. Additional contributions will require further review or approval by SMCSO and each Party.

All data, including replications, shall be deleted by SMCSO from all shared data repositories within 48 hours of a written request by a Party.

F. Additional Agencies:

Each Party grants authority to SMCSO to execute information sharing agreements with other California law enforcement agencies, and to expand, incorporate, and unify additional shared information from other California Law Enforcement agencies, except where explicitly denied by the Party. SMCSO will notify Parties in advance of such changes for review and approval.

G. Sharing in Compliance with State and Federal Law

In gathering, sharing, and storing information, and in all other respects in performing acts related to this Agreement, the Parties will comply with Section IV, above, all applicable laws, rules, and regulations, both those in existence at the time of execution of this MOU and those enacted subsequent to execution of this MOU, including but not limited to, to the extent applicable, the California Values Act (Government Code Section 7284 *et seq.*). SMCSO will, consistent with

Government Code Section 7284.8(b), ensure that any database is consistent with the Attorney General's guidance, audit criteria, and training recommendations which require that the databases are governed in a manner that limits the availability of information therein to the fullest extent practicable and consistent with federal and state law, to anyone or any entity for the purpose of immigration enforcement.

No party shall disclose contributed data pursuant to a subpoena, court order or other discovery request without (1) prior timely notification to the Party who is the official custodian of the contributed data, (2) engaging in reasonable and good faith efforts with the requester of the information and the custodian Party to limit disclosure of the contributed data.

H. Ownership of Contributed Data

Each Party retains ownership and control over its contributed data. Any request for information, including but not limited to inquiries under the California Public Records Act, will be directed to the Party that is the originator of the requested data.

V. COSTS

A. Operating Costs

Unless otherwise provided herein or in a supplementary writing, each Party shall bear its own costs in relation to this MOU and continued participation in or access to the data contributed by each Party. All obligations of and expenditures by the Parties will be subject to their respective budgetary and fiscal processes and subject to availability of funds pursuant to all laws, regulations, and policies applicable thereto. The Parties expressly acknowledge that this MOU in no way implies that any funds have been or will be appropriate for such expenditures.

VI. TERM OF AGREEMENT

A. TERM

This MOU shall be effective as of the last signature date of all Parties and will remain in effect until and unless it is terminated. This MOU will be reviewed every three (3) years thereafter for updates and consistency with applicable statutes and policies.

B. WITHDRAWAL

Any Party may withdraw from this MOU upon ninety (90) days' written notice to all other Parties. Upon withdrawal, the Party's access to data and contributed data, shall also be terminated. All rights, obligations, responsibilities, limitations, and other understandings with respect to the disclosure and use of all information received during a Party's participation in this MOU shall survive any withdrawal.

In the event one Party withdraws their participation from this MOU, this MOU shall survive and continue to be fully effective and binding on the remaining signatories.

VII. TERMINATION

This MOU will terminate automatically if two (2) or more Parties have withdrawn their participation from this MOU. All Parties will receive written notice within thirty (30) days of the second Party's withdrawal.

Upon termination of this MOU, each Party's access to data and contributed data shall also be terminated. All rights, obligations, responsibilities, limitations, and other understandings with respect to the disclosure and use of all information received during each Party's participation in this MOU shall survive any termination.

VIII. INDEMNIFICATION

Notwithstanding the provisions of Government Code Section 895.2, each Party shall defend, indemnify, and hold harmless other Parties (as well as their officers, agents, employees and representatives) from any and all losses, liability, damages, claims, suits actions and administrative proceedings resulting from the indemnifying Party's own acts or omissions (including those of its officers, agents, employees or representatives) arising out of relating to the performance of any of the provisions of this MOU. Parties do not assume liability for the acts or omissions of persons other than their respective officers, agents, employees, and representatives.

IX. SIGNATORIES NOT AGENTS

Parties of this MOU shall have no authority, express or implied, to act on behalf of another Party's signatory in any capacity whatsoever as an agent. The Parties shall have no authority, express or implied, pursuant to this MOU to bind each other to any obligation.

X. ASSIGNMENTS

Parties to this MOU may not assign any right or obligation pursuant to this MOU. Any attempted or purported assignment of any right or obligation pursuant to this MOU shall be void and of no effect.

XI. AMENDMENTS

This MOU may be amended by a written document signed by all Parties.

XII. SEVERABILITY

If any provision of this MOU is found by any court or other legal authority, or is agreed upon by the Parties, to be in conflict with any law or regulation, then the conflicting provision shall be considered null and void. If the effect of nullifying any conflicting provision is such that a material benefit of this MOU to a Party is lost, then the MOU may be terminated at the option of the affected Party, with the notice required in Section VI. In all other cases, the remainder of this MOU shall be severable and shall continue in full force and effect.

XIII. NO THIRD-PARTY BENEFICIARIES

This MOU is intended solely for the benefit of the Parties to this MOU. Any benefit to any third party is incidental and does not confer on any third party to this MOU any rights whatsoever regarding the performance of this MOU. Any attempt to enforce provisions of this MOU by third parties is specifically prohibited.

XIV. WAIVER

A waiver by a Party of a breach of any of the covenants to be performed by another Party shall not be construed as a waiver of any succeeding breach of the same or other covenants, agreements, restrictions, or conditions of this MOU. In addition, the failure of any Party to insist upon strict compliance with any provision of this MOU shall not be considered a waiver of any right to do so, whether for that breach or any subsequent breach. The acceptance by a Party of either performance or payment shall not be considered a waiver of the performing or paying Party's preceding breach of this MOU.

XV. AUTHORITY OF SIGNATORY TO BIND ENTITY

By signing below, each signatory warrants and represents that he/she/they executed this MOU in his/her/their authorized capacity and has legal authority or has received such authority from the Party, to bind the Party. This MOU may be executed in counterparts.

IN WITNESS WHEREOF, the Parties have executed this MOU by the signatures of the fully authorized representative of each Party.

Signed:

Name:

Title:

Agency: