INTERGOVERNMENTAL AGREEMENT
FOR INFORMATION SYSTEMS SERVICES IN PUBLIC SAFETY
between
the City of Flagstaff, Coconino County, and
Arizona Board of Regents
for and on behalf of
Northern Arizona University

This intergovernmental agreement ("Agreement") is entered into this ___ day of _____, 2023, between the CITY OF FLAGSTAFF ("CITY"), an Arizona municipal corporation, with offices at 211 W. Aspen Avenue, Flagstaff, Arizona, COCONINO COUNTY, ("COUNTY") a political subdivision of the State of Arizona, with offices at 219 East Cherry Avenue, Flagstaff, Arizona 86001, and the Arizona Board of Regents, a body corporate with perpetual succession pursuant to the laws of the State of Arizona, acting for and on behalf of NORTHERN ARIZONA UNIVERSITY ("NAU"), a public institution of higher education, with an address of PO Box 4124, Flagstaff, Arizona 86011.

RECITALS

A. The CITY, COUNTY and NAU (which may be referred to herein as a "PARTY" or the "PARTIES") each operate their own public safety computer network and have benefited over recent years from sharing access to the Criminal Justice Information System ("CJIS") Servers, joint access servers, and joint access databases under a prior IGA.

B. The PARTIES now desire to enter into this updated Agreement to reconfigure the roles and responsibilities of the PARTIES with respect to these joint access servers and joint access databases.

C. It is in the best interest of the citizens of Flagstaff and Coconino County for the PARTIES to share resources, information and costs of operation to provide more efficient and cost-effective solutions for public safety information needs.

D. The CITY and COUNTY have entered into a separate agreement for the transfer of the COUNTY's NORAZ domain, including physical infrastructure, to the CITY's control and possession. As of fiscal year 2022, physical and logical migration of CITY Police infrastructure commenced. Since that time the CITY and NAU have had access to the COUNTY's enterprise network. Until the NORAZ migration is complete, the CITY and NAU will continue to have access to the COUNTY'S Enterprise Network.

E. The CITY has access to COUNTY hosted shared systems and information technology ("IT") infrastructure at Law Enforcement Administrative Facility ("LEAF") , such as, but not limited to, closed circuit television ("CCTV"), and badge readers. This access is at the sole discretion of the COUNTY.

F. The PARTIES are authorized to enter into Intergovernmental Agreements pursuant to A.R.S. §§ 11-952 and 41-2631 et seq.

NOW, THEREFORE, in consideration of the promises and mutual covenants contained herein, the PARTIES agree as follows:

1. Purpose

The purpose of this Agreement is to provide a technical framework that allows for data sharing and cost sharing of public safety information across the named PARTIES.
(See **Appendix A**, for specific PARTY responsibilities regarding data integrity.)

2. Scope

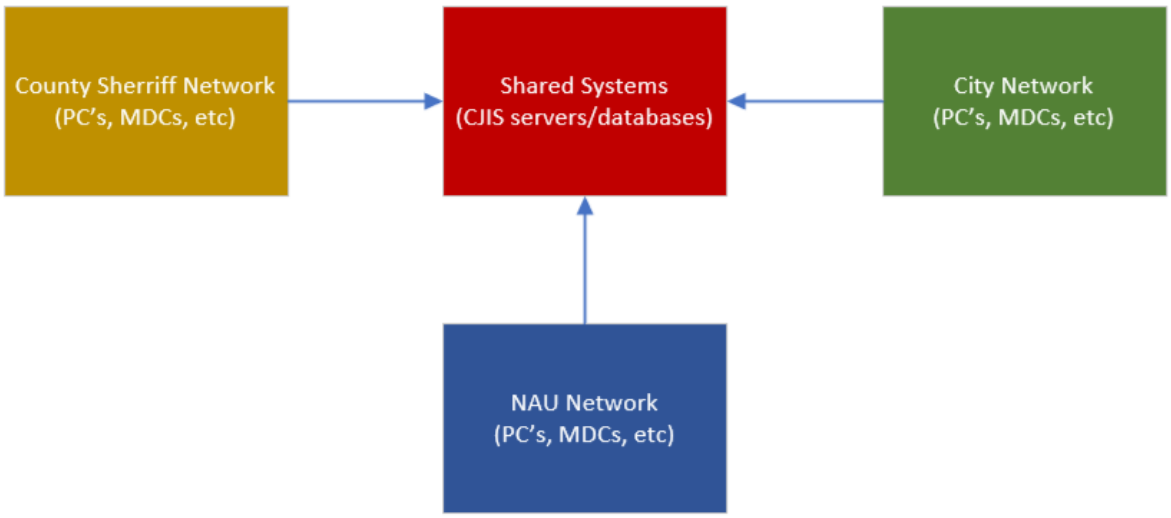
2.1 Definitions of shared systems

Shared Systems - Any servers, networking, databases, or other data or infrastructure for the purpose of this Agreement to facilitate data sharing between PARTIES. See "Network Layout" section for a diagram. Shared systems include the below listed elements.

Computer Aided Dispatch (CAD) - The dispatch software.
Records Management System (RMS) - The records software. Includes the Jail Management System (JMS)
(See **Appendix A, B, C and D and H** for additional definitions and descriptions of shared systems and data, PARTY responsibilities, and non-shared systems and data)

2.3 **Network Layout:** The following diagram is a simplified shared network diagram. All co-managed servers and shared data is stored in a centralized network. The PARTIES manage their end-user devices in their own network but connect to the shared/co-managed servers, databases.

*Note: This diagram is illustrative only. It does not capture all technology or configurations within the various networks.



2.4 **Rights and Responsibilities of All PARTIES: Shared Systems**
-Administrative logical and physical access to all shared systems

-Ability to audit or request 3rd party audit of all shared systems be agreed upon by Criminal Justice Information Services ("CJIS") compliant auditor.
- The PARTY who is the primary support agency will be responsible for remediation within 30 days unless otherwise agreed upon for critical life safety applications.

ALL PARTIES agree to full read access to any owned data in the "Shared System" infrastructure covered under this Agreement, unless access is limited due to Internal Affairs or on-going investigation.

2.5 **General Operations - Responsibilities of PARTIES: COUNTY Hosted Shared Systems**

All PARTIES will comply with all COUNTY IT governance, risk, and compliance policies while accessing COUNTY networks. It is the responsibility of all PARTIES to ensure their vendors comply with COUNTY governance, risk, and compliance policies while accessing COUNTY networks.

2.6 **General Operations - Responsibilities of PARTIES: Shared Systems**

All PARTIES will bear full responsibility for their employees, officers, and agents use of any of the shared systems. Each PARTY (as "indemnitor") agrees to indemnify, defend, and hold harmless the other PARTIES (as "indemnitee") from and against any and all claims, losses, liability, costs, or expenses (including reasonable attorney's fees) (hereinafter collectively referred to as "claims") arising out of bodily injury of any person (including death) or property damage but only to the extent that such claims which result in vicarious/derivative liability to the indemnitee, are caused by the act, omission, negligence, misconduct, or other fault of the indemnitor, indemnitor's officers, officials, agents, employees, or volunteers.

One PARTY will be listed as a primary support for each particular system or device. Each PARTY will have the capability and responsibility to create and maintain its own user accounts on each of the shared systems as needed. (See **Appendix A** for primary support responsibility for various interfaces.)

All infrastructure inventory of shared infrastructure devices will be maintained by the PARTY acting as the primary support agency and include the following information:

- Estimated replacement costs of equipment for budgeting purposes
- Refresh Cycle (See **Appendix B** for equipment refresh period.)
- Purchase Date
- Primary Support PARTY
- Additional Configuration Information as needed

Backups (See **Appendix D** for backup responsibilities)

- Primary backups will be stored onsite
- Secondary and tertiary backups may be stored offsite. If redundant backup sites are at PARTY locations, escorted access will be provided to all PARTIES upon request.

Software Contracts

- Subject to Section 3 of this Agreement, City of Flagstaff will pay for the cost of software maintenance, licensing and upgrades and invoice other PARTIES per this Agreement for their share of the costs. (See **Appendix G** for how cost sharing is calculated.)
  -

Miscellaneous Responsibilities

- This Agreement recognizes that technology may change over time and this Agreement may not cover all technology upon initial creation. The PARTIES agree to meet and discuss any new technology that is being considered and the responsibilities that come with that prior to acquiring such technology. Any newly acquired technology will be added to the Agreement by an Amendment to the Agreement when it is acquired. Shared technology will be proposed and approved by all PARTIES, including timeline, dependent systems, available resources, and budgetary requests.
- See **Appendix D** for Miscellaneous Responsibilities and the primary support PARTY or owner for miscellaneous items or technologies.

2.7 **Responsibilities of PARTIES: Non-Shared Systems Migrated to the City of Flagstaff**

CITY will be the sole responsible entity for cyber security/privacy and cyber liability on non-shared CITY systems historically administered by the COUNTY Sheriff's Office on or before March 1, 2023 (See **Appendix H** for support responsibility of interfaces).

Rights and Responsibilities of ALL PARTIES (Respective PARTY Networks)
-Maintain all respective PC's, laptops, Mobile Data Computers (MDCs).
-Maintain all respective network equipment.
-Maintain all respective servers, storage, or other information systems infrastructure.
-Comply with security best practices including relevant Federal and State laws, public safety compliance guidelines and cyber-security policies governing the shared systems.
-All PARTIES will utilize federal best practices in order to provide a documented set of security guidelines for member PARTY networks to adhere to.
-Ability to request an audit of PARTY networks connecting to shared networks for security best practices.

2.8 **Responsibilities of PARTIES: GIS Data Sharing**

All PARTIES will provide and have access to relevant GIS data for the following purposes:

- State and Federal Compliance
- Any data that has a functional impact on public safety for 911 dispatch and emergency response.
- Limit data usage to 911 Dispatch and Emergency Response purposes only

(See **Appendix C** for specific data requirements and responsibilities.)

2.9 **Shared Systems Security**

All shared systems will be managed as a separate standalone network from any of the PARTIES. The shared systems network will treat all PARTY networks as if they were an

external "untrusted3" network from a security perspective. To that purpose, the shared systems network will be secured to the maximum possible extent while providing only the necessary access to authorized users of each PARTY.

- Compliance: All PARTIES will comply with Arizona Criminal Justice Information System ("ACJIS") guidelines.
- Logging: Any access which PARTY member IT staff have will be with unique credentials and will be logged.

All PARTY administrative agents with access to the joint access systems will comply with the cyber-security and privacy policies of this Agreement. Failure to do so may result in revocation of individual administrative access. See **Appendix D** for cyber-security/privacy responsibilities.

2.10 **After Hours Support**

Each PARTY will provide 24 hour a day /7 days a week support for their respective systems identified in **Appendix A**.

Customers will be required to request after hours support from their PARTY IT support. If there is an issue that requires additional support from another PARTY IT department, the request will be made from the originating IT support staff and not directly from the customer.

2.11 **Change Control:** IT Support Staff from all PARTIES will follow a Change Control policy before any changes are made to joint access systems. (See **Appendix E** for Change Control Policy.)

2.12 **Problem Management:** All major infrastructure outages will be well documented per Problem Management policy. (See **Appendix F** for Problem Management Policy.)

3. Shared Systems Approvals and Funding

- All costs will be shared with all PARTIES. See **Appendix G** for how cost sharing is calculated.
- PARTIES will provide funding for all joint access network, server or other information systems infrastructure on the scheduled refresh date.
- PARTIES will provide funding for all shared software maintenance annually.
- All costs will be reviewed jointly by PARTIES on an annual basis and include the following year's cost estimates.
- All enhancements, software license agreements, and all other agreements related to this Agreement, and/or purchases will be proposed and not adopted until approved by all PARTIES
- All costs are subject to budget adoption by each respective PARTY.

4. Transfer of Infrastructure and Responsibilities

This Agreement replaces the previous agreement #A2005-0118 and associated amendments. As part of this change, COUNTY Sheriff transfers the following infrastructure to the CITY's sole control and all responsibilities associated with such infrastructure:

- All CITY Police PC's, laptops MDC's and other client access devices

- All Network Access Switches connecting to ports on the CITY police side of the shared public safety facility
- Any other computer infrastructure, network infrastructure or software applications solely used and accessed by CITY Police.

5. Confidentiality

The PARTIES shall comply with all applicable local, state, and federal confidentiality and privacy laws and regulations, including, but not limited to HIPAA. Nothing in this Agreement shall require or be construed to require any PARTY to violate such provisions of law or subject another PARTY to liability or render such PARTY to breach of this Agreement for adhering to such provisions of law. Confidential Information may include, but is not limited to personally identifiable health information, and other personally identifiable information such as financial, employment, or police records ("Confidential Information")

Confidential Information may be supplied to the PARTIES solely for the purposes of performance under this Agreement and PARTIES agree not to use this data for any other purpose or to disclose the data to any third party, other than as provided below. The PARTIES shall be liable for any damages arising from breach of any local, state, or federal confidentiality or privacy laws related to each PARTY's performance under this Agreement.

Each PARTY agrees to take all reasonable and appropriate action to prevent such disclosure by its employees or agents. The confidentiality covenants contained herein will survive the termination or cancellation of this Agreement. This obligation of confidentiality will not apply to information that:

i. is in the public domain, either at the time of disclosure or afterwards, except by breach of this Agreement by a PARTY or its employees or agents;

ii. a PARTY can establish by reasonable proof was in that PARTY's possession at the time of initial disclosure;

iii. a PARTY receives from a third PARTY who has a right to disclose it to the receiving PARTY; or

iv. is the subject of a court order, subpoena, or other legitimate disclosure request or demand under the Arizona Public Records Law, A.R.S. § 39-121 et. seq.or similar applicable public disclosure laws governing this Agreement; provided, however, that in the event you receive a public records request, subpoena or other similar applicable request or demand, you will give the PARTY which owns the data prompt notice and otherwise perform the functions required by applicable law.

Any violation by a PARTY of any provision under this Confidential Information section shall constitute a material breach of this Agreement, and as such the other PARTIES reserve the right to exclude that PARTY from this Agreement or to terminate the Agreement immediately without penalty and pursue any remedies allowed by law to prevent or remedy a breach by a PARTY of its obligations to the Confidential Information section to include injunctive relief.

6 Indemnification

The CITY will be the sole PARTY responsible for cyber security and cyber liability during the migration of NORAZ, once the City has domain administrative authority. During the migration, the CITY shall indemnify, defend and hold harmless the other PARTIES, their members, directors, officers, employees, agents, attorneys and assigns from and against any and all claims, losses, liability, costs or expenses resulting from the negligent, reckless, or intentional wrongful conduct of the CITY, its members, directors, officers, employees, agents, attorneys and assigns while maintaining access to COUNTY enterprise networks or LEAF infrastructure. This indemnification shall survive termination of this Agreement or the termination of the participation of any of its PARTIES. The amount and type of insurance coverage requirements set forth in this Agreement shall in no way be construed as limiting the scope of the indemnity in this paragraph.

In all other events, circumstances, or occurrences other than those addressed by the preceding paragraph, the following dual indemnification provision shall apply. To the fullest extent permitted by law, each PARTY to this Agreement shall indemnify, defend and hold harmless the other PARTIES, their members, directors, officers, employees, agents, attorneys and assigns from and against any and all claims, losses, liability, costs or expenses resulting from the negligent, reckless, or intentional wrongful conduct of the indemnifying PARTY or PARTIES. This indemnification shall survive termination of this Agreement or the termination of the participation of any of its PARTIES. The amount and type of insurance coverage requirements set forth in this Agreement shall in no way be construed as limiting the scope of the indemnity in this paragraph.

ALL PARTIES shall provide evidence of cyber security insurance at the time the IGA is executed initially and on an annual basis.

7. Workers' Compensation Claims

The PARTIES shall comply with the provisions of A.R.S. §23-1022 (E) by posting the public notice required. As provided for in A.R.S. §23-1022(D), an employee of a public agency who works under the jurisdiction or control of or within the jurisdictional boundaries of another public agency pursuant to a specific intergovernmental agreement or contract entered into between the public agencies is deemed to be an employee of both public agencies. However, the primary employer is solely liable for the payment of Workers' Compensation benefits. As such, each PARTY shall maintain Workers' Compensation insurance coverage on all of its own employees providing services pursuant to this Agreement.

8. Insurance

Each PARTY shall bear the risk of its own actions and shall maintain Cyber Liability in an amount not less than Two Million Dollars ($2,000,000) per occurrence/Two Million Dollars ($2,000,000) aggregate with a retroactive liability date (if applicable to claims made coverage) the same as the effective date of the Agreement or earlier. The policy shall contain an Extended Claim Reporting Provision of not less than two years following termination of the policy. Self-insurance by the State of Arizona shall be acceptable equivalent of this for NAU. Nothing in this Agreement shall be construed as a waiver of any limitation on liability that may apply to a PARTY.

9. Effective Date; Term; Renewal

9.1 Effective Date. This Agreement will become effective for each PARTY after approval by its governing body (the "Effective Date").

9.2 Term. Except as otherwise provided in this Agreement, this Agreement will terminate on December 31, 2037.

9.3 Any PARTY may terminate its participation in this Agreement by providing the other PARTIES one hundred and eighty (180) days written notice.

9.4 Annually, the PARTIES will conduct a review of all appendices and any upcoming financial obligations due to infrastructure replacements or software upgrades. Every 3 years, the PARTIES will conduct a review of the entire Agreement and may make changes through an amendment signed by all PARTIES or terminate the Agreement.

9.5 This Agreement may be renewed through an amendment signed by all PARTIES for additional fifteen year periods.

10. Cancellation for Conflict of Interest

This Agreement is subject to cancellation for conflict of interest pursuant to A.R.S. § 38-511.

11. Compliance with All Laws.

Each PARTY shall comply with all federal, state, and local laws applicable to its organization, rules and regulations.

12. Execution Procedure

This Agreement will be executed in counterparts by the governing body of each PARTY.

13. Non-Discrimination.

Each PARTY warrants that it complies with any state and federal laws, rules and regulations which mandate that all persons, regardless of race, color, creed, religion, sex, genetic information, age, national origin, disability, familial status or political affiliation, shall have equal access to employment opportunities, including but not limited to the Americans with Disabilities Act. Each PARTY shall take affirmative action to ensure that it will not participate either directly or indirectly in the discrimination prohibited by or pursuant to Title VI of the Civil Rights Act of 1964, Section 504 of the Rehabilitation Act of 1973, Section 109 of the Housing and Community Development Act of 1974, the Age Discrimination Act of 1975, Genetic Information Nondiscrimination Act of 2008.

14. Legal Arizona Workers Act Compliance.

The PARTIES are required to comply with A.R.S. §41-4401, and hereby warrant that they will, at all times during the term of this Agreement, comply with all federal immigration laws applicable to the employment of their respective employees, the requirements of A.R.S. §41-

4401, and with the e-verification requirements of A.R.S. §23-214(A) (together the "state and federal immigration laws"). The PARTIES further agree to ensure that each subcontractor that performs any work under this Agreement likewise complies with the state and federal immigration laws.

A breach of a warranty regarding compliance with the state and federal immigration laws shall be deemed a material breach of the Agreement and the PARTY who breaches may be subject to penalties up to and including termination of the Agreement.

Each PARTY retains the legal right to inspect the papers of any contractor or subcontract employee working under the terms of the Agreement to ensure that the other PARTIES are complying with the warranties regarding compliance with the state and federal immigration laws.

15. Non-appropriation.

This Agreement shall be subject to available funding for each PARTY, and nothing in this Agreement shall bind any PARTY to expenditures in excess of funds appropriated and allotted for the purposes outlined in this Agreement.

16. No Third-Party Beneficiaries.

The PARTIES acknowledge and agree that the terms, provisions, conditions, and obligations of this Agreement are for the sole benefit of, and may be enforceable solely by, the PARTIES, and none of the terms, provisions, conditions, and obligations of this Agreement are for the benefit of, or may be enforced by, any person or entity not a party to this Agreement.

17. Records and Retention Requirements.

The PARTIES shall retain all records related to this Agreement, and each PARTY shall have the right to inspect all records of the other PARTIES pertaining to the Agreement. The PARTIES shall retain all records related to this Agreement for a minimum of five (5) years following completion of the Agreement. Such records may also be audited by the Auditor General of the State of Arizona. This record retention requirement shall remain in effect five (5) years following expiration of this Agreement.

18. Governing Law.

This Agreement shall be construed under the laws of the State of Arizona and shall incorporate by reference all laws governing intergovernmental agreements and mandatory contract provisions of state agencies required by statute or executive order. All statutes and regulations referenced in this Agreement are incorporated herein as if fully stated in their entirety in the Agreement. Each PARTY agrees to comply with and be responsible for the provisions, the statutes, and the regulations set out in this Agreement.

19. Dispute Resolution.

In the event of a dispute regarding the terms or the interpretation of this Agreement the PARTIES will consult with each other, in good faith, in an effort to settle the dispute. If the

PARTIES are unable to settle the dispute, the PARTIES may terminate this Agreement. As required by A.R.S. § 12-1518, the PARTIES agree to make use of arbitration in disputes that are subject to mandatory arbitration pursuant to A.R.S. § 12-133.

20. Amendments.

This Agreement cannot be modified or changed except by a written instrument executed by authorized representatives of all PARTIES.

21. SIGNATURES

Each PARTY represents and warrants that all necessary approvals for this Agreement have been obtained, and the persons whose signatures appear below have the authority necessary to execute this Agreement on behalf of the PARTIES indicated.

IN WITNESS WHEREOF, the PARTIES have caused this Agreement to be executed as of the day and year first above written.

ARIZONA BOARD OF REGENTS FOR AND ON BEHALF OF NORTHERN ARIZONA UNIVERSITY

Signature:_____
Name:_____
Title:_____
Date: _____

REPRESENTING NORTHERN ARIZONA UNIVERSITY
The undersigned counsel for Northern Arizona University has reviewed the Agreement and determined that the Agreement is in proper form.

Signature:_____
Name: Michelle G. Parker
Title: General Counsel
Date: _____

CITY OF FLAGSTAFF

_____
Name: Becky Daggett
Title: Mayor
Date: _____

REPRESENTING CITY OF FLAGSTAFF:
The undersigned counsel for the City of Flagstaff has reviewed the Agreement and determined that the Agreement is in proper form.

Signature:_____
Name:_____
Title:_____
Date:_____

COCONINO COUNTY

_____
Patrice Horstman
Chairman, Board of Supervisors
Date:_____

Attest:

_____
Lindsay Daley
Clerk of the Board
Date:_____

REPRESENTING COCONINO COUNTY:
This Agreement has been reviewed pursuant to A.R.S. §11-952 by the undersigned attorney who has determined that it is in proper form and is within the powers and authority granted under the laws of the State of Arizona to the Coconino County Board of Supervisors.

Signature:_____
Deputy County Attorney
Date:_____

Appendix A - Shared System Responsibilities

Software	Description	Vendor	Primary Support Agency	Backup Support Agen	Maintenance Cost	Upgrade Cycle (yrs)	Estimated Upgrade Cost	Amortized Upgrade Cost
Computer Aided Dispatch (CAD)	The 911 dispatch system including 911 GIS map updates.	Hexagon	COF	CCSO	$ 172,997	4	$ 750,000	$ 187,500
*Fire Departments	Blue Ridge Fire, Flagstaff Fire, Forest Lakes, Highlands, Pinewood, Summi	Hexagon	COF	CCSO				
*Law Enforcement Agencies	FPD, NAUPD	Hexagon	COF	CCSO				
Informer	Links with DPS for criminal history	Hexagon	COF	CCSO	TBD / PARTIES	TBD / PARTIES	TBD / PARTIES	TBD / PARTIES
Mobile for Public Safety (MPS)	Mobile Interface for CAD for patrol and fire	Hexagon	COF	CCSO	TBD / PARTIES	TBD / PARTIES	TBD / PARTIES	TBD / PARTIES
Firelink & Mediview	CAD Interface with Firehouse/ESO	Hexagon	COF	CCSO	TBD / PARTIES	TBD / PARTIES	TBD / PARTIES	TBD / PARTIES
FlowMSP	CAD Interface with Pinewood Fire, Flagstaff Fire, Summit Fire	Hexagon	COF	CCSO	TBD / PARTIES	TBD / PARTIES	TBD / PARTIES	TBD / PARTIES
Ipage	CAD Interface SMTP Relay to Cell Phones	Hexagon	COF	CCSO	TBD / PARTIES	TBD / PARTIES	TBD / PARTIES	TBD / PARTIES
Recommended Unit Service	CAD Interface for Closest Fire Unit to Incident	Hexagon	COF	CCSO	TBD / PARTIES	TBD / PARTIES	TBD / PARTIES	TBD / PARTIES
Tracker	CAD Interface for tracking MDCs location	Hexagon	COF	CCSO	TBD / PARTIES	TBD / PARTIES	TBD / PARTIES	TBD / PARTIES
Crime Reports	Online web reports Crime Mapping for FPD	Hexagon	COF	CCSO	TBD / PARTIES	TBD / PARTIES	TBD / PARTIES	TBD / PARTIES
Records Management System (RMS)	Stores all records. CAD pushes data to RMS.	Hexagon	CCSO	COF	$ 75,000	8	$ 725,000	$ 90,625
Jail Management System (JMS)	Part of the RMS but specific to the Jail	Hexagon	CCSO	COF	TBD / PARTIES	TBD / PARTIES	TBD / PARTIES	TBD / PARTIES
CopLink	Regional inter-agency criminal record database	Forensic Logic	COF	CCSO	TBD / PARTIES	TBD / PARTIES	TBD / PARTIES	TBD / PARTIES
Justice Web Interface (JWI)	Connection to State DPS for CJIS access	Arizona DPS	CCSO		TBD / PARTIES	TBD / PARTIES	TBD / PARTIES	TBD / PARTIES
E-Citation (CJI)	Part of the JWI connection for citations	Pragmatica	CCSO		TBD / PARTIES	TBD / PARTIES	TBD / PARTIES	TBD / PARTIES
AFIS Fingerprinting / LE Web	Fingerprinting & Law Enforcement Web mug shot repository	Arizona DPS	CCSO for connection		TBD / PARTIES	TBD / PARTIES	TBD / PARTIES	TBD / PARTIES
TRACS	Online traffic ticketing system	Arizona DOT	CCSO (future split)		TBD / PARTIES	TBD / PARTIES	TBD / PARTIES	TBD / PARTIES

Appendix B - NORAZ Infrastructure Refresh Cycle

Model	Description	Purchase Year	Refresh Cycle	Replacement Year	Replacement Cost	Amortized Annual Cost
C9300	CJIS Network (core)	2022	5	2027	13985	2797
C9300	CJIS Network (core)	2022	5	2027	13985	2797
R740xd	CADARC01	2021	4	2026	11500	2875
R740xd	CADDB1	2021	4	2026	11500	2875
R740xd	CADDB2	2021	4	2026	11500	2875
R640	CADINT01	2021	4	2026	9500	2375
R640	CADINT02	2021	4	2026	9500	2375
R640	CADTEST01	2021	4	2026	7500	1875
R640	CADTRAIN01	2021	4	2026	7500	1875
R640	MOBCOM01	2021	4	2026	7500	1875
R640	MOBCOM02	2021	4	2026	9500	2375
R730xd	RMSDB1	2021	4	2026	TBD / PARTIES	TBD / PARTIES
R530	RMSCOM1	2021	4	2026	TBD / PARTIES	TBD / PARTIES
R530	RMSAPP1	2021	4	2026	TBD / PARTIES	TBD / PARTIES
R730xd	RMSDB2	2021	4	2026	TBD / PARTIES	TBD / PARTIES
R530	WEBRMS	2021	4	2026	TBD / PARTIES	TBD / PARTIES
R640	TRACS (host)	2020	4	2024	33500	8375
R440	CJIS DC #1	2019	4	2023	5000	1250
VM	CJIS Veeam	2022	1	2023	5500	5500
DD3300	CJIS Backup storage	2020	4	2025	55000	13750
	Netwrix Auditor	2022	1	2023	4500	4500
FTD 2110	CJIS Firewall	2022	5	2027	6040	1208
FTD 2110	CJIS Firewall	2022	5	2027	6040	1208

* Replacement Cost as of 2022

Appendix C - GIS Data Responsibilities

Description	Data Owner
Addresses	Each Respective Entity
Centerlines	Each Respective Entity
Buildings	Each Respective Entity
Encumbrance / Rights of Way	Each Respective Entity
Land Ownership	County IT
Municipal Boundaries	County IT
Fire Districts	County IT
Parcels	County IT
Subdivisions	Each Respective Entity
Mile Markers	County IT
ESN	COF
ESZ	COF
CON	COF
Special Addresses	COF
Common Place Names	COF
MSAG	Dispatch Coordinator
Data Requests	Each Respective Entity
Quarterly / Next Gen Standard Map Rolls	COF
Stich Points	COF
Annexations	COF
NAU Data	NAU

Appendix D – Miscellaneous Responsibilities

This Appendix covers responsibilities that don't fit neatly under other sections.

Cyber-Security and Cyber-Liability

The CITY will be the sole PARTY responsible for cyber security and cyber liability during the migration of NORAZ. Following completion of the migration, dual indemnification clause shall apply to ALL PARTIES.

The CITY will maintain access to all Cyber-Security tools, data and reports including but not limited to firewalls, malware detection/prevention, vulnerability scanning and other tools.
In the event of a breach or suspected cyber security or privacy breach observed by any PARTY, all PARTIES agree to report the incident to all other PARTIES within 4 hours of the incident. The CITY will be responsible for forensic analysis of a breach and will provide a report to all PARTIES within 48 hours of completion. The CITY will be fully responsible for remediation and response including any applicable Federal and State laws.

Network Equipment
Due to the nature of network equipment in relation to Cyber-Security, the CITY will maintain primary responsibility for basic upkeep and maintenance of the joint access network equipment. Other PARTIES will have access to the configuration and administrative functions of the network equipment per the agreement.

Backups
Backups will be maintained by the COUNTY Sheriff on an interim basis, for all data within the Shared Network, until 30 days after the completion of the migration. The CITY will be responsible for the Backups from that time forward. All PARTIES will have access to the shared data backups but may not have access to the core backup system until it is migrated to a new shared managed system.

Data Integrity Specialist
The COUNTY Sheriff will maintain the responsibility and staffing for ensuring data integrity in the Shared Systems.

VoIP Paging
The COUNTY Sheriff will maintain support for the facility overhead paging system and the integration of that paging system into the CITY's VoIP system.

1. All PARTIES shall limit access among its staff to only those whose job function requires it and only to the components of the Shared Systems areas needed and shall at least quarterly review such internal authorized user lists to update as appropriate. Separations from employment should result in the immediate shut down by a PARTY of a prior authorized user's credentials to access the Shared System.

2. Individual PARTIES Subject to Annual Audit for Adherence to Required IT Security Measures

   a) Each PARTY to this Agreement shall be subject to audit by the CITY IT Security Officer to verify its adherence to the minimum cyber security requirements outlined in this Agreement. A finding of failure to adhere to these requirements, shall constitute a material breach of this Agreement such that the PARTY in noncompliance shall have their access to the Shared Systems blocked by CITY IT until the noncompliant PARTY achieves compliance and this has been verified by the CITY IT Security Officer.

   b) The CITY shall establish, maintain and upgrade as needed the Shared Systems infrastructure, both hardware and software, along with needed connectivity. CITY IT shall allow access to the Shared Systems by approved vendors in a timely manner for needed maintenance, repairs or expansion of the system as determined by the PARTIES, and in accordance with the ACJIS Security Policy.

VIII. Notification Required by PARTIES for Cyber Incident(s) Which May Affect Shared Systems

1. Each PARTY shall be responsible to notify the Other PARTIES within 4 hours of any known or suspected cyber security or privacy breach involving its own internal network, or emanating from its own elected officials, officers, employees or volunteers, whether or not known to have affected the Shared Systems, and to quarantine its internal network from the Shared Systems should this occur, until cleared by ALL PARTIES .

Appendix D - Misc Responsibilities

Description	Owner
Cyber-Security	COF
Cyber-Liability Insurance	COF
Network Equipment	COF
Backups	COF
Data Integrity Specialist	CCSO
VoIP Paging	CCSO

Appendix E - CJIS Change Control Policy

Request for Change

All changes to CJIS co-managed infrastructure will be communicated via email to all agencies. This email will include the proposed change, the reason for change, and a backout plan.
All changes will apply an analysis and approval process based on the criteria below.

Change Definitions

- **Priority** = How soon the Change needs to be completed
  - **Urgent** = Must be completed immediately
  - **High** = Must be completed within the next couple weeks
  - **Medium** = Should be completed but no strict timeframe
  - **Low** = If not completed, it wouldn't have a large negative effect
- **Impact** = How many people the Change may affect
  - **High** = Nearly the entire organization
  - **Medium** = A group of people (i.e. a department or team)
  - **Low** = The change implementer and up to one other person
- **Risk** = Likelihood of a failure and/or difficulty recovering in case of unexpected issues
  - **Very High** = Unknown change and/or complete failure in case of issues (no recovery options)
  - **High** = Complex change and/or major failure in case of issues (full restore needed)
  - **Medium** = Common task (though may not have been done before) and/or simple back out plan (basic restore needed)
  - **Low** = Routine Task (similar task done before) and/or easy back out plan
- **Change Type**
  - **Standard** = We have an existing documented process (Low Risk and Low Impact)
  - **Minor** = Risk and/or Impact are Medium or lower
  - **Major** = Risk and/or Impact are Medium or higher
  - **Emergency** = Priority must be Urgent. This is almost always in response to a critical system failure that needs to be addressed immediately.

Change Approval Process

Standard Changes can be performed without any formal CAB approval. Only an email communicating the change is required. A Standard Change MUST have a CAB approved fully documented process and this process must be followed. This encourages staff to create documentation for regularly performed tasks.
Minor Changes can be approved via email as needed rather than waiting for a CAB meeting. A Minor change will be defined as a rating of one Medium/Low rating and one Low rating for Risk and Impact.
Major Changes would have any rating of Medium (or greater) for both Risk and Impact. These will be discussed and agreed upon at a CAB meeting.
Emergency Changes would be due to an outage or other emergency. Emergency Changes do require communication of the change but can be acted upon without CAB review. A detailed after-action report will be provided at a subsequent CAB meeting as to why the Emergency Change was needed.

Roles and Responsibilities

Change Advisory Board (CAB)

The CAB meeting will meet every other week to discuss changes. Additionally, the CAB meeting will be a time to review completed changes, failed changes, and old/delayed changes with lessons learned. Finally, the CAB meeting will be a place to discuss improvements to the change process.

Regular members of the Change Advisory Board include at least one person from each Agency. Additionally, the Change Requestor and any relevant personnel to the change will be invited to the CAB meeting.

Project Management

In some instances, a request may be large enough in scope or cost that it requires additional conversation and planning. The CAB meeting may be used as a way to request a larger project or initiative. In this case, a meeting will generally be scheduled to include both IT and business stakeholders from all PARTIES to discuss the costs, staffing commitments and other considerations before implementing a change or project. Any PARTY may request this further review for such a change request.

Appendix F - CJIS Problem Management Policy

Definition of a Problem

A Problem is an Infrastructure Outage that affects multiple users and/or departments.

Problem vs Incident/Ticket

An "Incident" or "Ticket" is a single event usually related to a single user. If multiple users experience the same interruption of IT Services, it then becomes a problem. A problem differs from an Incident in several key ways:

- A problem almost always requires escalation from Help Desk to higher level support.
- A problem often affects multiple people and may have multiple incidents/tickets associated.
- A problem often requires a change to the infrastructure to provide the fix.

Problem Process

During a Problem event, IT staff will make a determination as to which PARTY holds primary responsibility for resolution of the Problem. If the PARTY not responsible for the infrastructure receives a report from their staff regarding a Problem, they will reach out to the appropriate PARTY using each PARTIES process.

Upon initial resolution of the Problem, the supporting PARTY will inform all relevant stakeholders and PARTIES of the Problem resolution and any needed workarounds.

Step 2 – Root cause analysis

A root cause analysis will need to be completed following any Problem. This analysis can occur immediately following the Problem resolution or at the next convenient business day.
Results from the root cause analysis will be communicated to all stakeholders via email upon completion and discussed at the next Change Advisory Board meeting. The PARTIES will work to provide remediation to mitigate future Problems of a similar nature.

Appendix G – Cost Sharing

Costs for maintaining the public safety software systems will be split based on the following methodologies:

By User Count – This methodology splits costs based on the number of users (usually defined by number licenses) utilizing a system. This methodology is best used for software maintenance costs and network infrastructure costs. It generally is the default methodology when other methodologies don't fit well.

By Number of MDC's – This methodology is used for MPS and I Tracker, MDC interfaces with CAD

By Number of Seats – This methodology is used for CAD and interfaces from CAD to RMS

By Number of users of On-Call – This methodology is used for RMS and interfaces with CAD

By IT Efforts – This methodology splits costs by number of tickets, problems, changes or other statistics to show level of effort differences between agencies. The intent of the IGA is to share responsibilities so that IT efforts offset each other, but this methodology may be used in annual reviews to shift responsibility or adjust cost sharing as necessary.

In the first year of this agreement (July 1, 2022 thru June 30, 2023), all costs of the shared network **will be split based on the methodologies outlined above** unless otherwise agreed upon by each party at the time of purchase. In subsequent years, this appendix will be modified as necessary as part of an annual review.

Appendix H - Non-Shared Systems Migrated to the City of Flagstaff

Software	Description	Vendor	Support Agency	Migration Status	Maintenance Cost	Upgrade Cycle (yrs)	Estimated Upgrade Cost	Amortized Upgrade Cost
ESRI support of all CAD, Vesta, & Dispatch supported users	Map Roll, Mapping, and Data Support	ESRI	COF	COMPLETE	TBD / PARTIES		TBD / PARTIES	TBD / PARTIES
Vesta Phone 9-1-1	Shapefiles for Vesta 9-1-1 phone systems	ESRI	COF	COMPLETE	TBD / PARTIES		TBD / PARTIES	TBD / PARTIES
*Law Enforcement Agencies	FPD, NAUPD, Page PD, Sedona PD, Williams PD	ESRI	COF	COMPLETE	TBD / PARTIES		TBD / PARTIES	TBD / PARTIES
*National Parks	Grand Canyon National Park, Glen Canyon National Park	ESRI	COF	COMPLETE	TBD / PARTIES		TBD / PARTIES	TBD / PARTIES
Dispatch Map Support	Shapefiles for Dispatch when requested	ESRI	COF	COMPLETE	TBD / PARTIES		TBD / PARTIES	TBD / PARTIES
*Medical Response Agencies	Guardian Medical	ESRI	COF	COMPLETE	TBD / PARTIES		TBD / PARTIES	TBD / PARTIES
Verint Recorder / Goserco	Radio and phone recordings for CAD	Verint	COF	COMPLETE	TBD / PARTIES		TBD / PARTIES	TBD / PARTIES
Motorola Radios	Dispatch Radios PD and NAU	Motorola	COF	COMPLETE	TBD / PARTIES		TBD / PARTIES	TBD / PARTIES
BlueTeam / IA Pro	Manage Citizen Complaints and Internal Affairs Investigation	IA Pro	COF	COMPLETE	TBD / PARTIES		TBD / PARTIES	TBD / PARTIES
Intelligent Video Solutions	Interview Room IP Cameras & Server	Intelligent Video Solutions	COF	COMPLETE	TBD / PARTIES		TBD / PARTIES	TBD / PARTIES
AWACS Department of Homeland	NAU PD and FPD	DOHS	COF	COMPLETE	TBD / PARTIES		TBD / PARTIES	TBD / PARTIES
Amber Alert System	NAU PD and FPD	State of AZ	COF	COMPLETE	TBD / PARTIES		TBD / PARTIES	TBD / PARTIES
Silent Witness	Comes through Dispatch	County Attorney	COF	COMPLETE	TBD / PARTIES		TBD / PARTIES	TBD / PARTIES
Police Reports.US	Part of webRMS interface for public to access police reports	Police Reports.US	COF	COMPLETE	TBD / PARTIES		TBD / PARTIES	TBD / PARTIES
CarFax for Police	Part of webRMS interface for FPD	CarFax for Police	COF	COMPLETE	TBD / PARTIES		TBD / PARTIES	TBD / PARTIES
Bair Analytics	Part of webRMS for FPD Crime Analyst	Bair	COF	COMPLETE	TBD / PARTIES		TBD / PARTIES	TBD / PARTIES
Evidence.com	Axon/Taser and Body Cams	AXON	COF	COMPLETE	TBD / PARTIES		TBD / PARTIES	TBD / PARTIES
AdobePro	Adobe Professional Licensing	Adobe	COF	COMPLETE	TBD / PARTIES		TBD / PARTIES	TBD / PARTIES
Criticall	Dispatch Testing Software	Criticall	COF	COMPLETE	TBD / PARTIES		TBD / PARTIES	TBD / PARTIES
VM	CJIS DC #2		COF	PENDING IGA/MIGRATION		Hosted on County VM.	Create as physical host on NORAZ or migrate to VM host	
VM	webrmstest		COF	PENDING IGA/MIGRATION		Hosted on County VM.	Create as physical host on NORAZ or migrate to VM host	
VM	LEAFNM - Netmotion Servier		COF	PENDING IGA/MIGRATION		Hosted on County VM.	Create as physical host on NORAZ or migrate to VM host	
VM	OCRREMOTE: RD for City Attorney and City Warrant Officers		COF	PENDING IGA/MIGRATION		Hosted on County VM.	Create as physical host on NORAZ or migrate to VM host	

Appendix I - County-Hosted Shared System Responsibilities

Vendor	Primary Support Agen	Backup Support Agen	Maintenance Cost	Upgrade Cycle (yrs)	Estimated Upgrade Cost	Amortized Upgrade Cost
Badge Pass	CCSO	COF	$ 2,500		TBD / PARTIES	TBD / PARTIES
WiseNet	CCSO Facilities	TBD / PARTIES	TBD / PARTIES		TBD / PARTIES	TBD / PARTIES
Velocity	CCSO Facilities	TBD / PARTIES	TBD / PARTIES		TBD / PARTIES	TBD / PARTIES

Appendix J – Other Expectations

Service Level Agreement

In the first year of this agreement (July 1, 2022 thru June 30, 2023), each party will work on a "best effort" basis for resolving issues. In future years, parties may agree to a more specific Service Level Agreement for response times on various issues.

Additional Expectations

Additional expectations may be agreed upon by all parties after an annual review of potential improvements, satisfaction, or issues that have occurred over the previous year.