# TALLAHASSEE POLICE DEPARTMENT
## GENERAL ORDERS

| | | | |
|---|---|---|---|
| | **SUBJECT**<br>Use of Artificial Intelligence | | |
| | **CHIEF OF POLICE**<br>*Signature on File* | | |
| **NUMBER**<br>79 | **ORIGINAL ISSUE**<br>05/15/2024 | **CURRENT REVISION**<br>N/A | **TOTAL PAGES**<br>4 |

### AUTHORITY/RELATED REFERENCES

FBI CJIS Security Policy
FDLE Guidelines for CJIS Access
Florida General Records Schedule GS-2
General Order 15, Facial Recognition Program
General Order 17, Records Management
General Order 56, License Plate Recognition System
General Order 77, Computer, Cellular Telephone and Data Utilization

### ACCREDITATION REFERENCES

CALEA Chapter None

CFA Chapter None

### KEY WORD INDEX

| | |
|---|---|
| **AI Vendor Requirements** | Procedure VII |
| **Breaches of Protected Information** | Procedure VI |
| **CJIS Security** | Procedure I |
| **Compliance Monitoring and Enforcement** | Procedure V |
| **Data Privacy and Retention** | Procedure II |
| **Training and Education** | Procedure IV |
| **Transparency and Accountability** | Procedure III |

### POLICY

It is the purpose of this policy is to establish guidelines for the Tallahassee Police Department regarding the use of artificial intelligence (AI) technologies to ensure compliance with the FBI CJIS Security Policy (CSP) and to safeguard the security of witness, victim, suspect, and intelligence data. The Tallahassee Police Department will

leverage responsible AI utilizing a Human in the Loop (HITL) approach to augment decision-making and automate workflows with AI-powered information and insights to ensure members do not violate the privacy and civil rights of individuals.

## DEFINITIONS

**Artificial Intelligence Systems**: Hardware, Software, or programs that have a component designed to mimic cognitive functions such as problem-solving, perception, and decision-making that are typically associated with human intelligence. These systems can be capable of analyzing large amounts of data, recognizing patterns, and making predictions or decisions based on that analysis. Examples of systems that utilize this technology are computer vision/video processing systems such as ALPR, Facial Recognition, and Briefcam, Natural Language Processing Systems (word to text programs or generative text) such as AXON Report Writer, Google Translate, ChatGPT, and analytical data collection systems such as CrimeView.

**Human in the Loop (HITL)** - Human-in-the-loop (HITL) is an iterative feedback process whereby a human (or team) interacts with an algorithmically generated system, such as computer vision (CV), machine learning (ML), or artificial intelligence (AI).

**LASO:** Local Agency Security Officer. A COT Technology & Innovations employee assigned to the Department who serves as the primary contact between the Department and the FDLE regarding the security of criminal justice information accessed via the COT computer network.

**Member**: any department employee who may be granted access to technology that utilizes artificial intelligence.

## PROCEDURES

### I. CJIS Security

1. All AI systems used by the Tallahassee Police Department must comply with the FBI CJIS Security Policy (CSP).

2. Prior to implementing any AI technology, the Tallahassee Police Department CJIS compliance officer (LASO) must conduct a thorough assessment to ensure compliance with CJIS standards, including but not limited to encryption, access controls, and auditing requirements as listed in General Order 77, CJIS Security Protocols.

3. Only authorized members with appropriate clearance levels shall have access to CJIS data processed or generated by AI systems.

## II. Data Privacy and Retention

1. AI systems used for data gathering, analysis, or dissemination must adhere to strict security protocols to prevent unauthorized access, modification, or disclosure of sensitive information.

2. The Tallahassee Police Department shall remain in control of all data generated by AI systems, except that which is releasable by law.

3. All data stored, transmitted, or processed by AI systems must be encrypted/stored securely to protect against interception or data breaches.

4. The Tallahassee Police Department shall ensure that the use of AI technologies complies with all applicable data privacy laws, regulations, and that data/information generated adhere to current state data retention timelines.

## III. Transparency and Accountability

1. Members of the Tallahassee Police Department shall be aware of the capabilities, limitations, and potential biases of AI technology.

2. The Tallahassee Police Department shall ensure that the use of AI technologies aligns with City of Tallahassee ethical standards. The Tallahassee Police Department encourages responsible use of these emerging technologies, and its members are accountable for the use of these tools.

3. Bias mitigation strategies to include HITL and personnel augmented decision making shall be implemented to minimize the risk of discriminatory outcomes in decision-making processes facilitated by AI systems.

4. Instances where AI systems are utilized to support case information or identify possible suspects will require independent, non-AI developed, facts or circumstances to give authority to detain or arrest.

## IV. Training and Education

The Tallahassee Police Department technology and Innovation LASO, who is responsible for developing, implementing, or overseeing AI initiatives in the Department shall receive training on CJIS compliance, security, and ethics.

## V. Compliance Monitoring and Enforcement

1. Compliance with this policy shall be monitored through annual audits, inspections, and reviews conducted by the TPD LASO.

2. This policy shall be subject to periodic review by the TPD LASO and revision to ensure its effectiveness, relevance, and alignment with evolving legal and technological landscapes.

## VI. Breaches of Protected Information

In the event of a notable cybersecurity incident or data breach Tallahassee Police Department shall provide a notification to the Cybercrime Office of the Department of Law Enforcement including the following:

1. A summary of the facts surrounding the cybersecurity incident or ransomware incident.

2. The date of the most recent backup; the physical location of the backup, if the backup was affected; and if the backup was created using cloud computing.

3. The types of data compromised by the cybersecurity or ransomware incident.

4. The estimated fiscal impact of the cybersecurity incident or ransomware incidents.

5. In the case of a ransomware incident, the details of the ransom demanded.

## VII. AI Vendor Requirements

In the event of the use of a third-party AI solution or service the vendor must adhere to the requirements below:

1. The vendor must have a cybersecurity framework in place such as NIST, ISO27001, SOC2, PCI DSS, etc.

2. The vendor must use industry standard and up-to-date security tools and technologies such as antivirus protections, antimalware, ransomware protections, and intrusive prevention and detection methods.

The vendor must encrypt all data used by AI system.