Austin Fire Department

"Our Mission Goes Beyond Our Name"

4201 Ed Bluestein, Austin, TX 78721
(512) 974-0130
www.austinfiredepartment.org

UNMANNED AERIAL SYSTEM/VEHICLE (UAS/UAV) DATA IMAGE STORAGE AND RETENTION POLICY

A. Data Images

a. All data images obtained during the course of UAS operation—including those acquired during training events—are the property of the Austin Fire Department except when the data is obtained at the request and on behalf of another agency as specified in Section V(6).

b. Request for copies of the stored data images shall require a written request from the requestor and will be reviewed prior to release by the Fire PIO and/or City of Austin Law Department pursuant to the AFD Public Information Request policy.

I. Definitions

Digital Electronic M**anagement System** (DEMS) is a content management system (CMS) that centrally stores and manages all digital files. It allows an organization to control and centralize management of digital content or data.

UAS/UAV (hereafter referred to as UAS): Unmanned Aircraft System and all of the associated support equipment, control station, data links, telemetry, communications, navigation equipment, etc., necessary to operate the unmanned aircraft {Federal Aviation Administration (FAA)}. For the purposes of this policy, "UAS" will encompass all unmanned rescue robotics operated by the AFD RED Team, including maritime and ground robots.

HD Camera: A High Definition (HD) activity image capture device designed for digital imagery photography and/or video.

The Robotics Emergency Deployment (RED) Team is comprised of members from the Austin Fire Department who are dedicated towards further evaluating and refining the use of robotics in the fire service and other public safety related fields. The overall mission of the RED Team is to mitigate real-world problems through the deployment and use of air, ground, and maritime remotely operated rescue robotics. Collectively, this team is made up of individuals that meet or exceed the FAA standards to operate a UAS.

A memory card (sometimes called a *flash memory card* or a *storage card*) is a small storage medium used to store data such as text, pictures, audio, and video for use on small, portable, or remote computing devices.

Digital Image is a numeric representation (normally binary) of a two-dimensional image. Depending on whether the image resolution is fixed, it may be of vector or raster type. By itself, the term "digital image" usually refers to raster images or bitmapped images.

Critical Data is that may be related to an investigation, involves a fatality, is part of critical government infrastructure, is related to an imminent threat to public safety, and/or has a potential terrorism or criminal nexus.

Non-Critical Data is that information gathered during the mission that is not deemed part of an investigation and/or involves a fatality.

II. Purpose:

To establish written policies and procedures for the storage and retention of digital imagery collected by the Austin Fire Department's Robotics Emergency Deployment (RED) Team. This policy applies to RED Team members who collect and submit digital imagery to the Fire Department's digital electronic management system (DEMS).

III. Background:

The vision of the Austin Fire Department's RED team is to enhance firefighter safety and improve emergency response protocols through training, reconnaissance, assessment, and implementation of emerging technologies. Such tools can help facilitate increased situational awareness and incident command decisions at emergency scenes. During the course of operations, the use of aerial systems can be utilized in circumstances that could save lives and/or property, as well as providing the capability to detect possible dangers to emergency crews that could not otherwise be seen.

Digital images collected during the course of training and operations are a critical resource for evaluating the effectiveness and efficiencies of RED Team procedures. Protocols must be in place to ensure data is properly managed and maintained with regard to security and storage of electronic images.

IV. Procedure:

The Fire Chief or his/her designee must approve any mission request in advance of a deployment. RED Team digital imagery will be used for official AFD business only unless another agency has requested the mission; the footage then becomes their property to do with as they see fit. Copies of RED Team digital imagery will not be made available unless and until the requestor is authorized to view the digital imagery and does not otherwise have access to RED Team data. This may include public information requests processed in accordance with AFD policy.

Digital images taken by RED Team members will be downloaded into the Fire Department's DEMS. All required information (meta-data tags) will be entered to ensure proper identification and that the chain of custody of images is maintained. These images will not be stored in any other unauthorized locations.

RED Team members will not post, transmit, or otherwise disseminate confidential or sensitive information, including pictures, evidence, or other materials relating to work assignment without express permission of the Fire Chief or his/her designee.

Mission requests must be made in writing via the Mission Request Form. No UAS will be deployed until the Mission Request Form has been approved by the Fire Chief or his/her designee. This protocol may be postponed or waived by the Fire Chief or his/her designee in the event of an emergency or as deemed necessary, but a Mission Request Form will still need to be filled out and signed off on for records retention purposes.

1. **Documentation and Storage of Electronic Data**
   - **a.** Equipment check and weather will be documented in the RED Team's logbook prior to all UAS operations.
   - **b.** After each flight, the operator will complete a statement documenting the UAS's operations.
   - **c.** After each deployment, all video obtained by the UAS will be submitted to the Fire PIO for inclusion in the DEMS.
   - **d.** All digital imagery shall be stored in accordance with department policy and procedures.
   - **e.** The operator of the UAS is responsible for electronic data handling as well as writing any supporting documentation for the incident.
   - **f.** Digital imagery may be temporarily stored on or accessed via a Fire Department computer to meet an operational need. Once the electronic data is no longer needed, the employee must remove the images from the Department computer and deliver them to the Fire PIO for DEMS storage.
   - **g.** Members will not store, transfer, or utilize electronic images and digital imagery for personal use.

2. **RED Team Normal Business Hours Deployment Operations:**
   - **a.** After the completion of on-scene flight operations, the RED Team member will transfer non-critical data to either the secure Fire Department G drive folder or deliver the memory card to Fire PIO during normal business hours for processing of digital imagery.
   - **b.** The data will be either downloaded from the G drive or removed from the memory card, and images contained therein processed into the DEMS system. The empty memory card (if applicable) will then be returned to the RED Team member.
   - **c.** The RED Team member or Fire PIO member will document that the digital imagery was either downloaded from the G drive or the memory card, or submitted to Fire PIO for upload into the Fire Department's DEMS.
   - **d.** If the digital imagery is related to an investigation, the RED Team member will report directly to Fire Investigations to ensure chain of custody and follow procedures related to, "**AFD Fire Investigations Section SOG Filing Room Procedures Document #C301."** The RED Team member shall then communicate with Fire PIO to inform them that the digital imagery has been delivered to Fire Investigations.

3. **RED Team After-Hours Deployment Operations:**
   - **a.** After the completion of on-scene flight operations, the RED Team member will either transfer non-critical data to either the secure Fire Department G drive folder or secure the memory card in a locked location until it can be delivered to Fire PIO during normal business hours for processing of digital imagery (but no later than 24 hours after completion of the mission).
   - **b.** The RED Team member will make arrangements to have the memory card delivered to Fire PIO at AFD HQ (if applicable) so the images can be downloaded into the DEMS. That information will be captured on the Fire PIO log. The empty memory card will then be returned to the RED Team member.
   - **c.** If the digital imagery is related to an investigation, the RED Team member will report directly to Fire Investigations to ensure chain of custody and follow procedures related to, "**AFD Fire Investigations Section SOG Filing Room Procedures Document #C301."** The RED Team member shall then

communicate with Fire PIO to inform them that the digital imagery has been delivered to Fire Investigations.

d. If the digital imagery is related to an investigation, it shall be retained at AFD Investigations until the investigation is completed or per Investigations' retention schedule.

4. Access and Use

a. Only authorized personnel, as determined by this policy and authorized by the Fire Chief or his/her designee, will be involved in, or have access to, UAS digital images.

b. Only the Fire Chief or his/her designee, Fire PIO, and Fire Investigations may authorize the release of UAS images.

c. All requests for release of UAS images must come from an official Public Information and/or legal request.

d. A log documenting access to and use of data stored on the Fire Department's DEMS will be maintained for a period of three months unless otherwise indicated.

e. See UAS Privacy Policy for further details.

5. Records Retention

a. All RED Team digital imagery shall be retained for a period of time that is consistent with the City of Austin's Record Management Ordinance, chapter 2-11, and any applicable City Records Control Schedule and/or the state or local Government Retention schedules, but for no less than a period of 90 days from the date the data was captured. For more information, see City code chapter 2-11(Records Management):http://www.austintexas.gov/edits/document.cfm?id=221538.

b. Prior to the disposal of any RED Team digital imagery, Fire PIO, AFD Investigations, and the City of Austin Law Department shall be consulted to ensure that the digital imagery is not the subject of a pending Public Information Act request, and/or has no evidentiary value in any pending or potential administrative, civil, criminal, or other legal proceeding.

c. Upon expiration of the applicable retention period, digital imagery stored on the DEMS will be disposed of unless retained as part of an investigation.

6. Data Requests for Information

a. Information relating to ongoing fire investigations will only be released following review and approval by a Fire Investigator.

b. Any agency who wishes to obtain a copy of the footage must follow the request protocol outlined in this policy. If the footage was collected at the request of an agency besides the Austin Fire Department, that agency must submit a written request to the Fire PIO to obtain the footage and then it will be released to that agency by the Fire PIO for them to distribute as they see fit.

c. Mission requests from other agencies will be reviewed by the Fire Chief or his/her designee. Digital imagery obtained during those missions will be placed on an external media device (i.e., flash drive) for release to the agency. AFD may, but is not required to, retain any copies of said footage.

d. The Fire PIO and/or Fire Investigations will review footage before release of data is granted. Some parts of video images not related to the incident and/or investigation may be redacted to protect privacy in compliance with HIPPA, or any other applicable State or Federal law.

e. Open Records Requests for recorded video must be in writing and forwarded to the Fire PIO.

f. Legal requests (e.g., subpoenas, search warrants, etc.) for recorded video must be in writing and forwarded to Fire Investigations.

g. Fire Investigations will be responsible for reviewing and responding to all subpoenas made requesting the release of digital imagery obtained through UAS operations.

7. Notice of Operations

Being transparent about UAS operations is critical to building trust with those affected by its deployment. AFD strives to inform the public of the RED Team's purpose and operations. The following protocols will be consistent with RED Team UAS deployments:

a. The Fire Chief or his/her designee will be responsible for notifying the City of Austin Assistant City Manager over public safety when UASs are being deployed.

b. Flashing lights (if provided) will be utilized on UASs to indicate operation and location in flight unless the Fire Chief or his/her designee determines doing so would jeopardize or compromise the deployment of the UAS in an incident involving an imminent threat to public safety.

c. When possible, Fire PIO will pre-announce UAS operations in the affected areas on social media and via traditional media outlets.

d. AFD will place "Austin Fire Department" logos on all UAS equipment.

e. All RED Team members will wear clothing consistent with the identification of Austin Firefighters and/or RED Team participation.

f. When possible, notification will be made to residents in the immediate area of UAS operations prior to deployment.

Use of Unmanned Aircraft ("Drones") While On Duty

An Unmanned Aerial Vehicle (UAV), commonly known as a drone, is an aircraft without a human pilot aboard. The flight of UAVs may be controlled with various kinds of autonomy: by a given degree of remote control from an operator, located either on the ground or in another vehicle, or fully autonomously, by onboard computers.

AFD personnel are strictly prohibited from operating these systems at AFD facilities, regardless of duty status. This includes not only the facility and the space contained inside but also parking areas, green spaces, remote worksites, etc., as well as the airspace above these locations, unless otherwise authorized.

According to the Federal Aviation Administration (FAA), which governs the use of Unmanned Aircraft Systems (UASs)—of which UAVs are a component—there are three types of operators. These include public, civil, and model aircraft. Firefighters who are at work and/or on city property are considered public operators and are defined as follows:

"A public aircraft is one that is only for the United States government or owned and operated by the government of a state, the District of Columbia, or a territory or possession of the U. S. or a political subdivision. Operators of public aircraft include DOD, DOJ, DHS, NASA, NOAA, state/local agencies and qualifying universities. Civil aircraft means other than a public aircraft.

"For public aircraft operations, the FAA issues a Certificate of Waiver or Authorization (COA) that permits public agencies and organizations to operate a particular aircraft, for a particular purpose, in a particular area. The COA allows an operator to use a defined block of airspace and includes special safety provisions unique to the proposed operation. COAs usually are issued for a specific period – up to two years in many cases."

By the nature of our employment, firefighters are restricted from flying while on duty and/or at AFD facilities without the above COA.

AUSTIN FIRE DEPARTMENT ROBOTICS - PRIVACY POLICY

I. PURPOSE STATEMENT

The AUSTIN FIRE DEPARTMENT (AFD) created the Robotic Emergency Deployment (RED) Team to enhance firefighter safety and improve emergency response through the assessment and implementation of emerging technologies, such as Unmanned Aerial Systems (UAS) (also known as Unmanned Aerial Vehicles, or UASs) and ground and maritime remotely operated rescue robotics, that are equipped with Thermal Imaging Cameras (TICs), air monitoring sensors, and/or mounted cameras. Such tools help facilitate effective response to citizens in distress by establishing contact and accelerating assistance and/or rescue, minimize threat and risk of injury to individuals or public safety personnel and personal and real property, and increase situational awareness, sharing of information, and incident command decisions among first responders at emergency scenes. The deployment and use of remotely operated rescue robotics is intended to protect individual privacy, civil rights, civil liberties, and promote governmental legitimacy and accountability.

The AFD's deployment and use of remotely operated rescue robotics is not intended for law enforcement purposes or intelligence gathering but may be used by the AFD in the investigation and prosecution of arson-related crimes. The deployment and use of an AFD UAS for a law enforcement or criminal intelligence gathering purpose other than an arson investigation (a suspicious activity that has a potential terrorism or criminal nexus or is relevant to the investigation and prosecution of suspected criminal activity, the justice system response, and the prevention of crime or is useful in crime analysis or in the administration of justice and public safety) is prohibited except as provided for in this Policy.

Possible scenarios that may benefit from the deployment of robotics are:

- High-Rise Fires
- Search and Rescue
- Hazardous Materials Investigation
- Flood Events
- Wildfires
- Commercial and Residential Fires
- Post-Fire Investigations (including arson investigations)
- Pre-Fire Planning
- Scene Mapping

The purpose of this Privacy Policy is to ensure that safeguards and sanctions are in place to protect the privacy, civil rights, and civil liberties of all individuals, and other protected interests, including those of organizational entities, as well as to protect the integrity of fire department criminal investigations of potential arson-related incidents. It is also the purpose of this Policy to ensure accuracy of information and compliance with applicable law as information is developed, collected, exchanged, stored, and released.

II. DEFINITIONS

UAS is the unmanned aircraft system and all of the associated support equipment, control station, data links, telemetry, communications, and navigation equipment, etc., necessary to operate the unmanned aircraft (Federal Aviation Administration (FAA)).

First Responder refers to those individuals who, in the early stages of an incident, are responsible for the protection and preservation of life, property, evidence, and the environment, including emergency response providers as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101)(includes Federal, State, and local governmental and nongovernmental emergency public safety, fire, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities), as well as emergency management, public health, clinical care, public works, and other skilled support personnel (such as equipment operators) that provide immediate support services during prevention, response, and recovery operations.

Information refers to digital imagery (may include data in other mediums) recorded or transmitted by a UAS. This digital imagery may include data about people, organizations, events, incidents, or objects.

Law, as used in this policy, includes any applicable local, state, tribal, territorial, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order, as construed by appropriate local, state, tribal, territorial, or federal officials or agencies.

Need to Know is established when, as a result of jurisdictional, organizational, or operational necessities, access to sensitive information is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information in the performance of a first responder, homeland security, or counter-terrorism activity.

Public includes:

(1) Any person and any for-profit or nonprofit entity, organization, or association;
(2) Any governmental entity for which there is no existing specific law authorizing access to this information;
(3) Media organizations; and
(4) Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the AFD.

Public does not include:

(1) Employees of the AFD;
(2) People or entities, private or governmental, who have legal authority to assist the AFD in the operation of the RED Team function, and
(3) Public agencies whose authority to access information gathered and retained by the AFD is specified in law.

Right to Know is established when, based on having legal authority or responsibility, or pursuant to an authorized agreement, an agency or organization is authorized to access sensitive information in the performance of a first responder, homeland security, or counter-terrorism activity.

III. POLICY APPLICABILITY AND LEGAL COMPLIANCE

A. The AFD shall make this policy available to the public through available resources, including the AFD and the City of Austin websites.

B. All personnel who provide services to the AFD RED Team or have access to information garnered by the RED Team shall be provided with an electronic copy of this policy and the AFD UAS Data Image Storage Policy. These personnel will be required to provide a written acknowledgement of receipt of these policies and agreement to comply with their applicable terms and conditions. Such acknowledgements will be maintained by the Professional Standards Office of the AFD.

C. All AFD personnel with access to RED Team information shall operate in compliance with applicable law protecting privacy, civil rights, and civil liberties, including, but not limited to the U.S. and Texas Constitutions, and state law, including, but not limited to the Texas Government Code Chapter 552 Public Information Act.

D. The AFD has adopted internal operating policies that comply with the applicable law cited above and this policy.

IV. GOVERNANCE AND OVERSIGHT

A. Responsibility for the operation of the RED Team is assigned to the Fire Chief or his/her designee.

B. The Fire Chief or his/her designee shall:

- **a.** Resolve conflicts or disputes that might arise related to policy or mission;
- **b.** Establish protocol concerning the treatment of violations of this Agreement;
- **c.** Control the dissemination of any information produced by the AFD RED Team, including specific alerts and bulletins to agencies inside and outside the region;
- **d.** Review and update this Privacy Policy annually, as needed, taking into consideration recommendations by the City of Austin Public Safety Commission, other interested parties, and changes in applicable law;
- **e.** Shall be responsible for notifying the City Manager's Office of all UAS deployments; and
- **f.** Shall provide an annual report to the City of Austin Public Safety Commission on the status and efficacy of this Privacy Policy.

C. The AFD Fire Chief will appoint a RED Team Director, who will be responsible for the day-to-day operations of the RED Team. The Director will establish needed procedures, practices, and protocols as well as use advanced software, information technology tools, and physical security measures to ensure information is accessed only by authorized personnel and are protected from unauthorized access, modification, theft or sabotage, whether internal or external, or disasters or intrusions by natural or human causes.

D. All allegations of a violation of this Privacy Policy shall be referred to and investigated by the AFD Professional Standards Office.

E. Individual users of the RED Team information remain responsible for the lawful and appropriate use of that information. Failure to abide by the restrictions and use limitations of that information may result in the suspension or termination of individual user privileges, disciplinary sanctions, or criminal prosecution.

V. COLLECTION LIMITATION

A. All information will be obtained lawfully and can only be used for an AFD business- related purpose. When applicable, information that has a law enforcement or criminal intelligence value to the AFD shall be collected in strict compliance with the Fourth Amendment of the United States Constitution and all other applicable federal, state, or local laws.

B. The AFD will not use nor allow its UAS to be deployed based upon religious, political, or social views or activities; participation in a particular organization or event; or race, color, national original, age, disability, sex, sexual identity, sexual orientation, or any other status protected under local, state, or federal law.

C. In the event that a first responder agency has reason to believe that there is an imminent threat to public safety, the AFD UAS may be deployed and used to assist in the response to that imminent threat with the permission of the City Manager or his/her designee. The use of an AFD UAS for purposes other than public safety must be approved in advance by the City Manager or his/her designee.

D. Upon receipt of information collected by the RED Team, RED Team personnel shall assess the information to determine or review its nature, usability, and quality (when applicable, Arson investigators will have access to this information to determine its evidentiary value).

E. At the time the decision is made by the RED Team to retain information, it will be labeled to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:

- **a.** Not interfere with or compromise pending criminal investigations; and
- **b.** Protect an individual's right to privacy, or their civil rights and liberties.

F. All labels assigned to existing information will be re-evaluated at such times when new information is added that has an impact on access limitations or the sensitivity of disclosure of the information, or there is a change in the use of the information affecting access or disclosure limitations such as a change in case status.

G. All information related to an investigation conducted by the AFD Investigations Division shall be maintained pursuant to existing AFD policies and procedures.

H. These safeguards are intended to ensure that information that could violate civil rights and civil liberties will not be gathered, documented, processed, and shared either intentionally or inadvertently.

I. The RED Team will keep a record of all information collected by a UAS.

VI. INFORMATION SHARING

A. Except as provided herein, access to information contained within the RED Team's database will be granted only to RED Team members, the AFD Public Information Office, AFD Investigators who are authorized peace officers under the Texas Code of Criminal Procedure, members of the Professional Standards Office, the AFD Fire Chief or his/her designee, and any other individual approved by the Fire Chief or his/her designee. Each individual user obtaining information will be required to acknowledge, in writing, that he/she remains solely responsible for the interpretation, further dissemination, and use of the information, and is responsible for ensuring that any information relied upon is accurate, current, valid, and complete, especially before any official action is taken in full or partial reliance upon the information obtained.

B. RED Team information will not be shared with other individuals or agencies unless there is a need and right to know the information in the performance of a public safety, law enforcement, homeland security, or public health activity. A log will be kept for a minimum of two years digital imagery access by or dissemination of information to all recipients of the information, including AFD employees.

C. Information released by AFD to another agency will be governed by the laws and rules governing the individual agencies in respect to such data, as well as by applicable law:

- **a.** Requests from a law enforcement agency, including the Austin Police Department, for RED Team information that is not related to an imminent threat to public safety, will not be released except upon the receipt of a

subpoena or court order, and only after review by the City of Austin Law Department.

b. Information gathered by an AFD UAS that is not related to an imminent threat to public safety and has an incidental/unintended law enforcement or criminal intelligence gathering value will not be released except upon the receipt of a subpoena or court order, and only after review by the City of Austin Law Department.

D. The AFD will not allow original materials gathered or collected under these policies to be removed from the RED Team database unless necessary to be used in accordance with this Privacy Policy or in accordance with applicable laws, records retention policies, subpoena, or court order.

VII. RECORD RETENTION

A. All RED Team digital imagery shall be retained for a period of time that is consistent with the City of Austin Records' Management Ordinance, Chapter 2-11, and any applicable Records Retention Schedule including the State of Texas State Library and Archives Commission Retention Schedule for Records of Public Safety Agencies.

a. Given that there is no are existing records retention period applicable to data obtained from a UAS, the AFD shall maintain UAS digital imagery for a period of ninety (90) days from the date the data was captured, except when the data is the subject of a pending Public Information Act request, or has evidentiary value in any pending or potential administrative, civil, criminal, or other legal proceeding When the records are related to a pending criminal investigation by the AFD or another law enforcement agency, the records retention period shall be that which applies to criminal investigation records.

VIII. DISSEMINATION OF INFORMATION

A. RED Team information will only be provided to authorized personnel. Unauthorized access or use to the RED Team's resources is prohibited. Unauthorized posting, transmission, or other release or dissemination of RED Team information is strictly prohibited without the permission of the Fire Chief or his/her designee. The RED Team Director reserves the right to restrict personnel from access to RED Team information, and to suspend or withhold the access rights of any individual violating this Privacy Policy. The Fire Chief shall be notified of any individual's restriction or suspension of access to RED Team information. Any use of the RED Team's information in an unauthorized or illegal manner will subject the individual user to denial of further use or access, disciplinary action, and/or criminal prosecution.

B. Information obtained from or through the RED Team will not be used or publicly disclosed for purposes other than as specified in this Privacy Policy. Information cannot be: (1) sold, published, exchanged, or disclosed for commercial purposes; (2) disclosed or published without prior approval of the RED Team Director; (3) disseminated to unauthorized persons; or (4) used in any way that is otherwise inconsistent with the statutes, rules, policies, or procedures that govern the RED Team.

C. Information that would interfere with or compromise pending criminal investigations shall not be disseminated publicly unless required by law and only after consultation with the City of Austin Law Department.

IX. PUBLIC INFORMATION REQUESTS

Public information requests submitted to the AFD for RED Team information must be reviewed by the AFD Public Information Officer. Requests for all other information maintained by the RED Team shall be handled in accordance with the procedures and legal requirements established under the Texas Public Information Act, Chapter 552 of the Government Code. The City of Austin's Law Department shall assist as needed concerning individual requests.

X. SECURITY SAFEGUARDS (See also AFD UAS Data Image Storage Policy)

A. The RED Team Director will also serve as the RED Team security officer. The security officer shall document and report internal and external breaches of security and violations of policy to the Fire Chief.

B. Access to RED Team information will be allowed only over secure networks or via external media devices as appropriate (i.e., external storage devices such as flash or hard drives).

C. The RED Team will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.

D. Except as provided herein, access to RED Team information will be granted only to RED Team assigned personnel whose positions and job duties require such access, and who have been selected, approved, and trained accordingly.

E. Queries made and access to the RED Team data applications will be logged into the data system identifying the user initiating the query.

F. Fire PIO and/or the RED Team will utilize documentation to maintain audit trails of requested and disseminated information.

G. When information has been breached or obtained by an unauthorized person and the release of such information may threaten physical, reputational, or financial harm to an individual or agency, the RED Team Director shall promptly notify the individual or agency, unless doing so would compromise an ongoing public safety operation or pending criminal investigation.

XI. COMPLIANCE, ACCOUNTABILITY, AND ENFORCEMENT

A. It is the intent of AFD to be open with the public concerning the use of UAS by the RED Team when such openness will not jeopardize ongoing public safety operations and/or arson-related investigative activities.

B. RED Team personnel or other authorized users shall report violations or suspected violations of this Policy to the RED Team Director within 24 hours of occurrence. The AFD Professional Standards Office shall be responsible for investigating all complaints of a violation of this Policy and shall report its findings to the Fire Chief.