flock safety

May 2021

Flock Safety CJIS Compliance Overview

Flock Safety's ALPR solution leverages plate number extract files from National, State, and local hotlist databases to provide real time alerting to Law Enforcement agencies with the goal of Eliminating Crime.

The most common hotlist extract file used with LPR solutions is the NCIC file provided by the FBI. This file is composed of hotlist entries submitted by agencies across the US and only contains license plate number and state, reason, vehicle description, and ORI number of the submitting law enforcement agency.

In order to access this file on behalf of a Law Enforcement agency, Flock Safety has read and understood the CJIS Security Policy (currently v5.9, dated 6/1/20) provided by the FBI. As a result, Flock Safety has implemented the necessary process and technologies to meet or exceed the "minimum standards of security requirements" outlined in the FBI's CJIS Security Policy.

The following document lays out the processes and technologies implemented by Flock Safety for compliance with the FBI's CJIS Security Policy. The following policy areas are as outlined in the CJIS Security Policy (v5.9).

As of May 2021, there is no central CJIS authorization body, no accredited pool of independent assessors, nor a standardized assessment approach to determining whether a particular solution is considered CJIS compliant. Flock Safety is committed to meeting CJIS requirements as published by the FBI.

Additional References

FBI CJIS Security Policy

Flock Safety Internet Security Policy

AWS CJIS Policy

flock safety

Policy Area 1—Information Exchange Agreements

As part of all Flock Safety contracts for service, whether as part of a purchase, trial, or shared access agreement*, Flock Safety and the agency enter into an “Information Exchange Agreement” in the form of a Memorandum of Understanding (MOU).

This MOU represents the commitment between the agency and Flock Safety to ensure prevention of unauthorized disclosure, alteration, or misuse of the CJIS data leveraged by the law enforcement agency via the Flock Safety solution.

**An agency who has not purchased Flock Safety cameras but has access to cameras purchased by another entity*

Policy Area 2—Security Awareness Training

All Flock Safety employees that interact with CJIS data or access infrastructure that handles CJIS data undergo the necessary Security Awareness Training, as well as a fingerprint-based background check. Additionally, these employees sign the FBI Criminal Justice Information Services Security Addendum.

Policy Area 3—Incident Response

Flock Safety is committed to the security of all customer data CJIS or otherwise. In the case of an incident Flock Safety defines its steps around reporting of accidental or malicious attacks that expose CJIS data. Flock Safety’s incident response policy is available publicly as part of the Flock Safety Internet Security Policy.

flock safety

Policy Area 4—Auditing and Accountability

Flock Safety is dedicated to the appropriate use of the Flock Safety technology by both Flock Safety customer users and Flock Safety employees. As a result, Flock Safety provides robust auditing that cover the events outlined in the FBI's CJIS Security Policy and more.

As part of these auditing events Flock Safety captures Date/Time, what was accessed, the type of access, who accessed it, and the outcome of that access. All audit information is stored for a minimum of 1 year, as outlined in the FBI's CJIS Security Policy.

Policy Area 5—Access Control

To ensure appropriate Access Control for both Flock Safety customer users and Flock Safety employees, Flock Safety has implemented granular access permissions that allow for the creation of roles associated with individuals based on the necessary control criteria set by the law enforcement agency under the CJIS policy.

All Flock Safety solutions hosted in AWS leverage AES 256 symmetric encryption in accordance with the CJIS Security Policy. Additionally, Flock Safety leverages FIPS 140-2-compliant APIs and storage in the AWS GovCloud. Flock Safety leverages secure, encrypted sessions to AWS servers using HTTPS (Transport Layer Security [TLS]).

Please see the AWS CJIS Compliance Overview for additional information.

Policy Area 6—Identification and Authentication

All Flock Safety users have a unique UUID (128-bit) that identifies them throughout the Flock Safety solution. This UUID is maintained even if changes are made to the user account (e.g., name change or permissions).

Flock Safety requires the use of secure passwords and provides multi factor authentication (MFA) solutions for additional security measures.

flock safety

Policy Area 7—Configuration Management

All changes to Flock Safety software and cloud hardware are logged and documented. Flock Safety leverages CJIS compliant hardware, with CJIS compliant access restrictions (physical and digital), which is hosted by AWS in their AWS GovCloud in the US.

Flock Safety maintains detailed network diagrams that outline the components of the Flock Safety system and the interactions between those components.

Please see the AWS CJIS Compliance Overview for additional information.

Policy Area 8—Media Protection

Flock Safety leverages CJIS compliant hardware, with CJIS compliant access restrictions (physical and digital), which is hosted by AWS in their AWS GovCloud in the US.

All Flock Safety solutions hosted in AWS leverage AES 256 symmetric encryption in accordance with the CJIS Security Policy. Additionally, Flock Safety leverages FIPS 140-2-compliant APIs and storage in the AWS GovCloud. Flock Safety leverages secure, encrypted sessions to AWS servers using HTTPS (Transport Layer Security [TLS]).

All Flock Safety license plate and image data is hard deleted based on the Flock Safety retention policy, or any democratically created retention policy by the agency.

Please see the AWS CJIS Compliance Overview for additional information.

Policy Area 9—Physical Protection

Flock Safety leverages CJIS compliant hardware, with CJIS compliant access restrictions (physical and digital), which is hosted by AWS in their AWS GovCloud in the US.

Please see the AWS CJIS Compliance Overview for additional information.

flock safety

Policy Area 10—Systems and Communications Protection and Information Integrity

Flock Safety leverages CJIS compliant hardware, with CJIS compliant access restrictions (physical and digital), which is hosted by AWS in their AWS GovCloud in the US.

All Flock Safety solutions hosted in AWS leverage AES 256 symmetric encryption in accordance with the CJIS Security Policy. Additionally, Flock Safety leverages FIPS 140-2-compliant APIs and storage in the AWS GovCloud. Flock Safety leverages secure, encrypted sessions to AWS servers using HTTPS (Transport Layer Security [TLS]).

Please see the AWS CJIS Compliance Overview for additional information.

Policy Area 11—Formal Audits

Flock Safety is ready to comply with and formal audits needed to ensure CJIS compliance.

Policy Area 12—Personnel Security

All Flock Safety employees that interact with CJIS data or access infrastructure that handles CJIS data undergo the necessary Security Awareness Training, as well as a fingerprint-based background check. Additionally, these employees sign the FBI Criminal Justice Information Services Security Addendum.

flock safety

Policy Area 13—Mobile Devices

Flock Safety solutions are cloud hosted and delivered as a web application. As a result, all Flock Safety solutions can be accessed by a computer or mobile device with a current generation web browser. As with any web-based application, the Flock Safety solution can be blocked or limited by any firewall or other security protocols implemented on law enforcement agency computers or mobile devices.

No matter the type of device, all Flock Safety solutions follow the necessary security protocols for access, audits, media protection, and overall security as covered in the proceeding Policy Areas.

Any requirements around the use of the Flock Safety solution via a mobile device shall be covered by the agency's CJIS policy, as is the case with any other computer owned/used by the law enforcement agency.