



## State of Minnesota Interconnection Security Agreement

SWIFT Contract No.: 282452

### Agreement Purpose

The purpose of this Interconnection Security Agreement (ISA) is to establish procedures for mutual cooperation and coordination between the Flock Group Inc. ("Flock") and State of Minnesota, Department of Public Safety, Bureau of Criminal Apprehension ("State of Minnesota" or "BCA"), together noted as "the parties," regarding the development, management, operation, and security of a connection between Flock and the BCA's Criminal Justice Data Communications Network for the benefit of Grand Rapids Police Department ("Governmental Unit").

This ISA is intended to minimize security risks and ensure the confidentiality, integrity, and availability of shared data and systems that have a network interconnection with Flock for the benefit of Governmental Unit. This ISA ensures the adequate security of shared data and systems being accessed and provides that all network access satisfies the requirements of the parties.

The guidelines establish information security measures that must be taken to protect the connected systems and networks as well as the shared data that traverses them, which includes FBI Criminal Justice Information (FBI CJI) that is accessed via the FBI's Criminal Justice Information Systems (FBI CJIS).

This ISA specifies business and legal requirements for the networks being interconnected and authorizes mutual permission to connect the parties and establishes a commitment to protect the connectivity between the networks, and shared data processed and stored on systems that reside on the networks.

Through this ISA, the parties must minimize the exposure of their connected systems and networks to security risks and aid in mitigation and recovery from security incidents.

This ISA covers the interconnection between the parties for the benefit of Governmental Unit.

Additional information on shared data and services that will utilize this connection can be found in the following documents: State of Minnesota Joint Powers Agreement Authorized Agency, executed between the State of Minnesota, acting through its Department of Public Safety, Bureau of Criminal Apprehension (BCA) and Governmental Unit, attached hereto as an addendum.

### Interconnection Purpose

The purpose of the interconnection is to provide Governmental Unit access to BCA systems and services as outlined in this Agreement through Flock's connection with the BCA. Flock and Governmental Unit entered into a separate agreement which governs the terms of that relationship.

### BCA & Governmental Unit

Under Minn. Stat. § 299C.46, the BCA must provide a criminal justice data communications network (CJDN) to benefit authorized agencies in Minnesota. Governmental Unit is authorized by law to utilize the CJDN pursuant to the terms set out in its joint powers agreement with the BCA. BCA either maintains

repositories of data or has access to repositories of data that benefit authorized agencies in performing their duties. Governmental Unit accesses these data in support of its official duties.

### **Entity Connecting to the State of Minnesota**

Flock is a public safety technology company offering Automated License Plate Reader (ALPR) Cameras and back end operating software that allows Governmental Unit to search for suspect vehicles and receive real time alerts to license plates associated with a criminal hotlist file.

This interconnection will provide Governmental Unit access to the following authorized BCA systems and services, including FBI systems and services, which include FBI CJI, provided through the BCA:

- 1) NCIC Hot Files
- 2) Stolen Vehicle file
- 3) Stolen License Plate file
- 4) Wanted Person file
- 5) Canadian Police Information Center (CPIC) Hot File Records (Wanted Persons, Stolen Vehicles, etc.)
- 6) Protection Order file
- 7) Missing Person file
- 8) Group Member Capabilities (part of the Violent Gang and Terrorist Organization file)
- 9) Supervised Release file
- 10) National Sex Offender Registry file
- 11) Immigration Violator file
- 12) Minnesota Hot Files
- 13) Minnesota Warrants file
- 14) KOPS Attempt to Locate Messages (Keep Our Police Safe (KOPS) alerts contain data from "attempt to locate" and "be on the lookout" messages to LEAs.
- 15) Minnesota License Plate Data File
- 16) Suspended driver licenses
- 17) Revoked driver licenses
- 18) Cancelled driver licenses
- 19) Disqualified driver licenses

### **Policies & Standards**

By interconnecting with Flock, the BCA and Governmental Unit agree to be bound by this ISA and the use of Flock and BCA Networks in compliance with this ISA.

In order to do so, Flock must comply with the following policies and agreements related to data provided by or through BCA systems and related to the BCA's CJDN, the terms of which apply to all sections within this agreement:

- 1) BCA MNJIS Policy 5000 – Appropriate Use of Systems and Data (Appendix C)
- 2) BCA MNJIS Policy 5002 – CJDN Network Security (Appendix C)
- 3) FBI CJIS Security Policy current and future updates (Appendix C)

If there is any conflict between policies, the minimum standard applied must be that of FBI and BCA policies. These BCA and FBI CJIS policies and regulations, as amended and updated from time to time, are incorporated into this Agreement by reference. These policies will be provided to the parties.

In order to comply with the policies and standards noted above, Flock attests to the following:

- 1) Flock utilizes a Memorandum of Understanding (MOU) to ensure prevention of unauthorized disclosure, alteration, or misuse of the FBI CJI leveraged by Governmental Unit via the Flock system.

- 2) All Flock employees with access to FBI CJI are required to complete an FBI fingerprint-based background check, CJIS Security Awareness Training, and sign the FBI CJIS Security Policy Security Addendum Certification.
- 3) Flock has defined an incident response policy and process for events that disrupt the confidentiality, integrity, or availability of CJIS data that includes notification of the BCA CJIS Systems Agency Information Security Officer (ISO) within 24 hours.
- 4) Flock adheres to the logging and auditing requirements set forth by the FBI's CJIS Security Policy current version and future changes for maintaining the required event logs for a minimum of one (1) year and reviewing them for anomalies on at least a weekly basis.
- 5) Flock has granular access permissions that allow for the creation of roles associated with individuals, based on least privilege as required by the CJIS Security Policy.
- 6) All Flock solutions are hosted in Amazon Web Service (AWS) and all CJI is hosted in the AWS Government Cloud (AWS GovCloud). These solutions leverage encryption of data at rest and in transit in compliance with the FBI CJIS Security Policy and BCA CJIS Network Security Policy. Additionally, Flock leverages NIST-certified FIPS 140-2 APIs and storage in the AWS GovCloud. Any system components that access, store, or transmit License Plate Reader file data must use the AWS GovCloud.
- 7) All Flock users have a unique UUID (128-bit) that identifies them throughout the Flock system. This UUID is maintained even if changes are made to the user account (e.g., name change or permissions).
- 8) All changes to Flock's software and hardware are logged and documented. Flock maintains detailed network diagrams that outline the components of the Flock system and the interactions between those components.

### **Scope of Agreement**

The scope of this ISA is based on the following, but not limited to:

Interconnection between the Flock network and the BCA.

Related network components belonging to the parties, such as hosts, routers, and switches; IT devices that assist in managing security such as firewalls, intrusion detection/intrusion prevention systems (IDS/IPS) that are associated with the network connection and shared data and systems between the parties.

### **Information Security**

The parties shall maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of the information contained on the system with the highest sensitivity levels. All security must be in compliance with all of the policies noted within this agreement.

The parties are responsible for coordinating with and reporting to both Flock's network and security operations center and the BCA Service Desk in the event of an IT security incident involving the services described in this ISA.

The parties are responsible for hardening, configuring, patching and otherwise maintaining hardware and software of systems managing this interconnectivity and supporting the other party's data (where relevant).

The parties must update their respective IT contingency plans to reflect this agreement. The parties shall share relevant sections of IT contingency plans with each other to ensure compatibility. The parties should include the other in relevant contingency plan testing, if appropriate.

The acting IT Managers of the parties will appoint Points of Contact (PoCs) to meet, or conduct a conference call, every year to review and discuss any changes to the IT security posture of the shared IT assets covered by this ISA, and any necessary changes to the IT security safeguards

### **Data & Network Security Controls**

Flock has deployed tooling across their AWS network, and all internal assets for continuous monitoring of indicators of compromise, vulnerabilities and configuration changes. Additionally, code is analyzed via SAST and SCA tooling prior to deployment. The application is continuously scanned via DAST tooling, and Flock participates in annual third-party penetration testing. All CJI is hosted within the AWS GovCloud.

Both the BCA and Minnesota IT Services (“MNIT”) have developed policies, standards, procedures, and guidelines to ensure the adequate protection of BCA data. Additionally, as the FBI’s identified CJIS Systems Agency (CSA) for Minnesota, the BCA is responsible for the security and appropriate use of FBI Criminal justice information in Minnesota. The BCA complies with the FBI CJIS Security Policy and BCA MNJIS Policy 5002 - CJDN Network Security. The BCA also enforces compliance with these policies for all Minnesota agencies who access BCA or FBI CJIS data.

MNIT monitors the BCA’s CJDN network twenty-four (24) hours a day, seven (7) days a week, i.e., 24/7, through automated monitoring. Both the BCA and MNIT provide and continually update awareness training for all users who have access to unencrypted BCA data or FBI CJI.

### **Connection Restrictions**

The parties shall:

- 1) Ensure that this interconnection traverses the Internet in an encrypted private tunnel using encryption that meets both the FBI and BCA standards.
- 2) Ensure that this interconnection is isolated and secure from all other customer / business processes.
- 3) Configure network perimeter security devices (firewalls, IPS/IDS, application firewalls, etc.) in accordance with BCA & FBI policies and requirements.
- 4) Block all network traffic incoming and outgoing, from, or to the Internet, Flock, BCA, or Governmental Unit unless it is explicitly permitted.
- 5) Install a firewall between the perimeter (demarcation point) of the BCA’s network and Flock network.
- 6) Maintain responsibility for configuring all network perimeter firewalls with a policy at least as stringent as the BCA’s.
- 7) Provide to Flock, through the Technical Point of Contact, a list of BCA hosts, servers and subnets permitted to traverse the interconnection, and the ports and protocols on which they operate.

### **Connection Diagram**

Appendix B of this ISA includes a topological drawing that illustrates the interconnectivity between both systems, including all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, source and destination IPs, IP Protocols and Ports). The parties shall notify each other of any requirements such as additional router connections or increases in volume associated with this ISA.

## **Service Level Agreements**

Flock's agreement with Governmental Unit is included as an addendum.

## **Roles & Responsibilities**

### **General**

Each party is responsible for assigning appropriate personnel to implement, configure and establish the outlined interconnectivity. This section describes specific roles and responsibilities required for this connectivity, and the communications expected between the parties.

### **Communications/ Points of Contact (PoCs)**

Appendix A is a list of the responsible parties for each system. Appendix A will be updated whenever necessary. Updating Appendix A does not require the re-signing of this ISA by either party. It is the responsibility of each respective approving authority to ensure the timely updating of Appendix A and for the notification of such changes to the alternate party within 30 days of any personnel change.

### **Technical Point of Contact (PoC)**

The parties will designate a technical lead for their respective network and provide PoC information to facilitate direct contacts between technical leads to support the management and operation of the interconnection;

- Maintain open lines of communication between PoCs at both the managerial and technical levels to ensure the successful management and operation of the interconnection; and
- Inform their counterpart promptly of any change in technical PoCs and interconnections.

### **Security Point of Contact (PoC)**

Flock will identify a Flock Information Security PoC to serve as a liaison between both parties and assist the State of Minnesota in consulting on security controls and requirements.

State of Minnesota will designate an Information Security PoC, the equivalent of the Flock Information Security PoC, who shall act on behalf of the State of Minnesota and communicate all security issues involving the State of Minnesota to Flock via the Flock Information Security PoC.

### **Network/Security Operations**

Flock's solution is hosted in AWS GovCloud. Their internal Security team is responsible for monitoring the network, in conjunction with other specific parts of the Engineering team. Flock's Security team operates normal business hours Monday - Friday from 9am to 5pm Eastern and is accessible via [security@flocksafety.com](mailto:security@flocksafety.com). Emergency escalations can be reported by calling 404-996-1905.

MNIT staff at the BCA provide support 7 a.m. – 5 p.m. Central Standard Time (CST) 10 hours a day, 5 days a week, Monday – Friday, with on-call support all other times. They can be reached at 888-234-1119 or [bca.servicedesk@state.mn.us](mailto:bca.servicedesk@state.mn.us). Security incidents can also be reported to the BCA Service Desk and should also be reported to the BCA Information Security Office at 651-793-2502 or [bca.iso@state.mn.us](mailto:bca.iso@state.mn.us).

The organization discovering a security incident will report it internally, in accordance with the organization's incident reporting procedures. Each organization will ensure that the other connecting organization is notified when security incidents may have affected the confidentiality, integrity or availability of the shared data or systems being accessed.

## **Events and Incidents**

The parties agree to abide by the communication requirements outlined for the situations specified below:

### **Security Incidents**

Both party's IT Managers will notify each other within two (2) hours by telephone or e-mail when a potential security incident involving a shared system or shared data is detected, so the other party may take steps to determine if its connected system or shared data has been compromised and to take appropriate security precautions.

### **Continuity of Operations Plan (COOP)/IT Disaster**

The parties shall immediately notify their designated counterparts, as defined in the information system contingency plan, in the event of a disaster or other contingency that disrupts the normal operation of one or both connected networks.

The IT Manager of either organization will notify their counterparts within four (4) hours by telephone or e-mail in case of a disaster, major equipment failure, or other event which requires the activation of a COOP or IT Disaster Recovery plan to restore IT systems or services for their respective organizations.

### **Configuration Change Control**

Planned technical changes to devices or systems that affect the connectivity described in this ISA will be reported to the counterpart IT Manager via e-mail at least one (1) month before such changes are implemented. The party implementing the change will update their counterpart at appropriate intervals, such as at initiation and completion of work efforts. Diagrams and documentation will also need to be updated at this time by the parties.

### **New Interconnections**

The initiating party notifies the other party at least one (1) month before it intends to permit any other traffic to traverse the same connectivity or tunnels established through this ISA. Any additional traffic must be approved by the BCA. Corresponding documentation and diagrams will be updated prior to implementation.

### **Personnel Changes**

The parties agree to provide notification of the separation or long-term absence of their respective PoC on a timely basis. In addition, the parties provide notification of changes in point of contact information, and update Appendix A within one (1) day of the change.

### **Data Categorization**

Data traversing this connection is provided by State of Minnesota to authorized users within the Governmental Unit. Controls for maintaining its confidentiality, integrity and availability of BCA and FBI data are the responsibility of State of Minnesota.

### **Encryption**

Data traversing this connection must be encrypted in compliance with the FBI CJIS Security Policy, BCA MNJIS Policy 5002 - CJDN Network Security, which requires that encryption in transit be secured with a NIST-certified FIPS 140-2 and or 140-3 encryption algorithm and that any weak or compromised ciphers are disabled. This requirement may change with any modifications to any of the policies noted within this agreement.

### **Audit Trail Responsibilities**

All parties are responsible for auditing equipment processes and administrative activities involving this Interconnection; as per their established policies and procedures. Activities that will be recorded should at least include: event type, event description, date and time of event, administrator identification, and equipment identification. All audit trails must be consistent with the policies noted in this agreement.

Auditing capabilities incorporate the assignment of responsibilities and segregation of duties, ensuring that appropriate records and documentation are maintained, consistent verification and review of procedures and access restriction guidelines.

The Joint Powers Agreement Section 7.1 describes the audit responsibilities of the BCA and the FBI CJIS division, including examining Flock books, records, documents, internal policies, and accounting procedure and practices.

### **Compliance**

If the BCA determines that Flock has jeopardized the integrity of the systems or tools covered in both this ISA and the JPA agreed to by Governmental Unit, the BCA may stop providing some or all of the systems or tools until the failure is remedied to the BCA's satisfaction.

### **Non-Disclosure**

State of Minnesota and Flock acknowledge that private, confidential, and/or security information might be generated or made available during the performance of this agreement. The parties specifically agree not to disclose any information received or generated under this agreement, unless its release is approved in writing by a Signatory Authority, as defined in Section 9. The parties further agree to assert any privilege allowed by law and to defend vigorously rights to confidentiality and security information for themselves. Neither party shall be responsible for the defense of the other.

### **Modifications**

The terms of this ISA shall remain in full force and effect, unless formally modified by the parties, or terminated by one. Any modifications shall require that the ISA be updated, approved and signed by the parties or their designees. Appendices may be modified as needed. Either party may terminate the ISA and the requisite connectivity at will.

### **Assignment**

If any term or condition of this ISA becomes inoperative or unenforceable for any reason, such circumstances shall not have the effect of rendering the term or condition in question inoperative or unenforceable in any other case or circumstances, or of rendering any other term or condition contained in this ISA to be invalid, inoperative, or unenforceable to any extent whatsoever. The invalidity of a term or condition of this ISA shall not affect the remaining terms and conditions of this ISA, unless agreed to by a Signatory Authority. Neither party may assign nor transfer any rights or obligations under this agreement.

### **Amendments**

Any amendment to this Agreement, must be in writing and will not be effective until all Signatory Authorities have signed and approved a written amendment.

### **Limitation of Liability**

Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall the State of Minnesota be liable to Flock or any other person for any indirect, special, incidental, or consequential damages of any character including, without limitation, damages for loss of

goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages.

**Waiver**

If the BCA fails to enforce any provision of this Agreement, that failure does not waive the provision or the BCA's right to enforce it.

**Venue**

The venue for all legal proceedings involving this Agreement, or its breach, must be in the appropriate state or federal court with competent jurisdiction in Ramsey County, Minnesota.

**Term & Termination**

The BCA may terminate this Agreement at any time, with or without cause, upon written notice to the Signatory Authorities. This agreement will automatically terminate five years from the effective date or on termination of the Flock service agreement with Governmental Unit, which is attached as an addendum to this agreement. If this agreement is terminated, any connectivity to the BCA will also be terminated immediately.

**THE BALANCE OF THIS PAGE INTENTIONALLY LEFT BLANK**

**Signatory Authority**

Signatory Authorities are individuals vested with the power to commit the authorizing organization to binding agreements, including this contract.

The parties agree to work together to ensure the joint security of the connected networks and the relevant data they store, process, and transmit, as specified in this ISA. Each party certifies that its respective network is designed, managed, and operated in compliance with this ISA. Each party also certifies that its respective network has been certified and accredited in accordance with each party's internal policies.

<b>Entity Connecting to the BCA</b> <b>Flock Group Inc</b>	
<b>Davis Lukens</b> <i>Chief Technology Officer</i> Flock Group Inc (with delegated authority)	Date
<b>Entity Benefitting from Connectivity</b> <b>Andy Morgan</b> <i>Chief</i> Grand Rapids Police Department (with delegated authority)	Date
<b>Tasha Connelly</b> <i>Mayor</i> City of Grand Rapids	Date
<b>State of Minnesota</b> <b>Kathryn Meiers</b> <i>Interim Deputy Superintendent of Minnesota Justice</i> <i>Information Systems</i> Minnesota Bureau of Criminal Apprehension	Date

## Appendix A

### BCA Contacts

#### **Interim Deputy Superintendent, BCA Minnesota Justice Information Services (MNJIS)**

**Name:** Kathryn Meiers

**Address:** 1430 Maryland Avenue East, St. Paul, MN 55106

**Voice Phone No.:** 651-793-2425

**E-mail Address:** [kathryn.meiers@state.mn.us](mailto:kathryn.meiers@state.mn.us)

#### **Deputy Director, MNJIS Technology**

**Name:** Stephanie Hoppesch

**Address:** 1430 Maryland Avenue East, St. Paul, MN 55106

**Voice Phone No.:** 651-793-2526

**E-mail Address:** [stephanie.hoppesch@state.mn.us](mailto:stephanie.hoppesch@state.mn.us)

#### **BCA Service Desk**

**Address:** 1430 Maryland Avenue East, St. Paul, MN 55106

**Voice Phone No.:** 888-234-1119

**E-mail Address:** [bca.servicedesk@state.mn.us](mailto:bca.servicedesk@state.mn.us)

#### **Technical PoC**

**Name:** Soua Yang

**Address:** 1430 Maryland Avenue East, St. Paul, MN 55106

**Voice Phone No.:** 651-793-2442

**E-mail Address:** [soua.yang@state.mn.us](mailto:soua.yang@state.mn.us)

#### **Security PoC**

**Name:** Thomas Miller

**Address:** 1430 Maryland Avenue East, St. Paul, MN 55106

**Voice Phone No.:** 651-793-2707

**E-mail Address:** [Thomas.miller@state.mn.us](mailto:Thomas.miller@state.mn.us)

### Flock Contacts

#### **Technical PC**

**Name:** Josh Collins

**Address:** 1170 Howell Mill RD NW Suite 210 Atlanta, GA 30318

**Voice Phone No.:** 1-866-901-1781

**E-mail Address:** [josh.collins@flocksafety.com](mailto:josh.collins@flocksafety.com)

#### **Security PC**

**Name:** Eric Tan

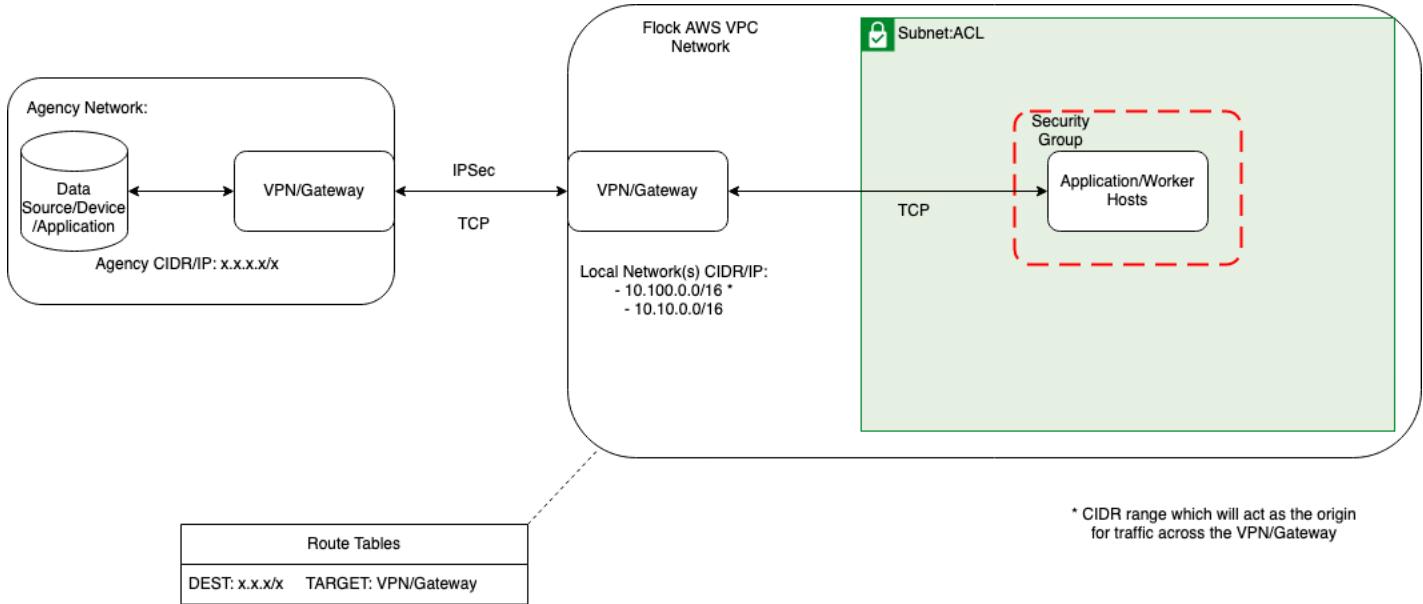
**Address:** 1170 Howell Mill RD NW Suite 210 Atlanta, GA 30318

**Voice Phone No.:**

**E-mail Address:** [eric.tan@flocksafety.com](mailto:eric.tan@flocksafety.com)

## Appendix B

### Image Describing Connectivity



## Appendix C

### Policies and Standards

#### **BCA MNJIS Policy 5000 Appropriate Use of Systems and Data**



BCA MNJIS Policy  
5000 - Appropriate U:

#### **BCA MNJIS Policy 5002 CJDN Network Security**



BCA MNJIS Policy  
5002 - CJDN Network

#### **FBI CJIS Security Policy**



FBI CJIS Security  
Policy v5-9-2\_202212C