Peregrine

PEREGRINE.IO

Attachment B

Security at Peregrine

At Peregrine, we recognize that true data security, privacy, and governance are non-negotiable when dealing with sensitive law enforcement data.

Our commitment to security goes beyond industry checkboxes; we invest in a proactive, multi-layered strategy that ensures data is not only protected from external threats but also governed internally with precision.

This white paper outlines the five pillars of the Peregrine security ecosystem:

1. **CJIS compliance**
   Always staying current with the latest national FBI CJIS standards for proper handling of criminal justice information (CJI)

2. **Identity management and authentication architecture**
   Moving beyond passwords to institutional identity integration

3. **Data encryption and residency**
   Ensuring encryption and residency standards meet or exceed the highest regulatory benchmarks

4. **Dynamic access control**
   Implementing a sophisticated data permissions model that evaluates not just who a user is, but the context and purpose of their request

5. **Auditability and transparency**
   Creating an immutable, transparent record of every action to ensure total auditability

By following the Principle of Least Privilege, Peregrine provides leaders with the confidence to empower their teams while maintaining control over their most sensitive information.

1. CJIS compliance

Law enforcement agencies handle sensitive CJI on behalf of the public, and Peregrine maintains full compliance with the latest version of the national FBI CJIS standard (as of this writing, Version 6, ref. NIST SP 800-53 Rev. 5).

- **Detailed, control-level documentation:** Peregrine maintains and continually updates detailed documentation on our implementation of the more than 180 controls that make up the CJIS standard. Peregrine provides this documentation to law enforcement agencies for review prior to making any network or system connections.
- **CJIS compliance hosting:** Peregrine is hosted in the secure, CJIS-compliant Amazon Web Services (AWS) Government Cloud Region (Gov Cloud).
- **Proven security to align with California DOJ standards:** Peregrine has been reviewed and approved to handle CJI by the California DOJ.
- **Additional security attestation:** Peregrine is also SOC 2 compliant, undergoing regular testing and third-party auditing to validate the implementation of our security controls. Peregrine can provide our latest SOC 2 attestation report upon request.

2. Identity management and authentication architecture

The entry point to the Peregrine platform is governed by rigorous authentication standards designed to eliminate unauthorized access at the perimeter.

- **Identity provider integration:** We prioritize Single Sign-On (SSO) as our primary authentication mechanism. The platform is built to integrate directly with customer identity providers via SAML, ensuring user identities are managed within the customer's own authoritative systems.
- **Multi-factor authentication (MFA):** For environments where SSO is not utilized, we enforce mandatory multi-factor authentication. Our current standard requires the use of token generators as the default MFA process to provide a higher security bar than traditional SMS or phone-based methods.
- **Network-level security:** We enable organizations to implement strict allow/deny lists that restrict platform access to specific, authorized email domains. Furthermore, administrators can configure approved organization subnets and IP ranges. Every login attempt is programmatically checked against these allow lists; requests originating from outside these approved environments are rejected by default.

3. Data encryption and residency

Peregrine's architectural approach to data protection is engineered to ensure the integrity and confidentiality of all hosted information.

Advanced encryption standards
Peregrine employs end-to-end encryption protocols to safeguard information against unauthorized access or interception. All cryptographic modules used within the platform are compliant with FIPS 140-2 (and 140-3), ensuring our encryption meets the stringent security requirements mandated for federal and highly regulated industries.

- **Encryption in transit:** All data transmitted over public or untrusted networks is encrypted using TLS 1.2 or higher. By utilizing FIPS-validated cryptographic algorithms, we ensure data remains protected from interception as it moves between the client and our infrastructure.

- **Encryption at rest:** All customer data stored within Peregrine's environment is protected at the storage layer using AES-256 encryption. This implementation relies on FIPS-compliant key management systems, ensuring that even in the event of physical hardware compromise, the underlying data remains inaccessible and cryptographically shredded.

Data residency and sovereignty
We recognize that the physical and logical location of data is a critical requirement for many of our clients.

- **Domestic server storage:** Peregrine supports data residency requirements by utilizing domestic server storage within the relevant jurisdiction. In the case of U.S. law enforcement customers, this means utilizing only U.S.-based server storage in the AWS GovCloud. This architecture ensures processing and storage occur within the legal and regulatory boundaries required by the client.

- **Secure infrastructure providers:** Peregrine leverages AWS GovCloud, which meets rigorous security and compliance standards including the physical security of data centers and background checks for personnel with physical access.

4. Identity management and authentication architecture

Our permissioning system enforces the Principle of Least Privilege, ensuring access is narrowly tailored to the user's specific operational needs. Peregrine offers a robust set of fine-grained access control policies that allow customers to choose what resources users can access, as well as how, when, where, and why that access is granted. These permissions also govern any potential authorized data sharing between law enforcement agencies. By default, any and all data sharing outside of an individual law enforcement agency is disabled. Law enforcement agencies have full control over whether they share data at all, with whom, and what specific types or elements of data are appropriate to share. Any and all data sharing and interactions with shared data are captured in granular audit logs, discussed further in Section 5.

Role-based access control (RBAC)
Initial access is determined by user-scoped roles — such as patrol, detective, or command staff — which define the baseline data models and features a user can interact with. This ensures permissions are aligned with the user's organizational function.

Attribute-based access control (ABAC)
To provide a more sophisticated layer of security for sensitive data, we implement attribute-based rules. These rules evaluate dynamic contextual factors at the moment of query execution, including:

- **Device security:** Verification that the user is accessing the system from an approved and secure device
- **Network context:** Validation of the user's current IP address against approved ranges

Purpose-based access control (PBAC)
For access to the most sensitive data sources, we implement and require a purpose-bound data session. This allows customers to align purpose with data control. A user may be granted access to sensitive data, but only for specified reasons.

Users must provide a specific reason for their access, selecting from an agency-defined list or providing a free-text justification. Results are only returned upon the submission of a valid reason.

Data-level granularity
Permissions are not limited to the dataset level; we also provide administrators with control at both the row and column levels. This includes:

- **Field-level redaction:** This grants the ability to hide specific sensitive attributes, such as Social Security Numbers, from broader view while still allowing users to see the rest of a record.
- **Action-specific permissions:** We explicitly separate the permissions for "view," "search," and "download." This distinction ensures a user may have the authority to discover a record without the technical ability to export it from the platform, mitigating the risk of bulk data dissemination.
- **User-scoped restriction:** We support dynamic permissioning where certain records (e.g., body camera footage) are only accessible if the user's unique login credentials match those linked to the data resource.

5. Auditability and transparency

All actions taken in Peregrine are logged in an immutable, transparent record that can be accessed at all times by organization administrators to ensure total auditability.

- **Immutable audit architecture:** Every meaningful action taken within the platform is captured in append-only audit logs. These logs are retained for at least one year and are accessible to administrators for active monitoring and alerting.
- **Easy and flexible audit searching:** Peregrine's audit log search user interface makes it easy for authorized customer administrators to search for logs from specific time periods, users, or even terms (e.g., searches for celebrity names).
- **Anomaly detection and alerts:** Administrators can utilize the platform's analytical tools to review logs and set push notifications for suspicious activities, such as:
  - Large-scale data exports
  - Repeated failed login attempts
  - Privilege escalations
  - Sharing with users from out-of-state jurisdictions