**Security**

**The EVIDENCE.com data security relies on the following elements:**

**Authentication:** The process of uniquely identifying the legitimate users of EVIDENCE.com. These include Officers, Administrators, Investigators, District Attorneys and other related law enforcement individuals. Only users with an active and legitimate username and password are allowed to access the EVIDENCE.com system.

**Authorization:** The process that governs the resources and operations that the authenticated user is permitted to access. Resources include Cases and Evidence such as video, audio, etc. Operations generally include transactions such as creating, authenticating, approving, editing, searching, archiving, sharing and deleting resources. Every EVIDENCE.com user is only allowed to access content and have access to actions as governed by the roles and security parameters established in the system and their agency policy.

**Auditing and Logging:** Auditing and logging is the key to non-repudiation. Non-repudiation guarantees that a user cannot deny performing an operation or initiating a transaction. In EVIDENCE.com this means every action performed on the system by an authenticated user is tracked and stored for future reference and system integrity. Every action and its details in the EVIDENCE.com system is maintained in a tamper-proof audit log, which is retained as long as the security guidelines dictate.

**Confidentiality:** The process of making sure that data remains private and confidential, and that it cannot be viewed by unauthorized users or eavesdroppers who monitor the flow of traffic across a network. Encryption is used to enforce confidentiality.

**Integrity:** The guarantee that data is protected from accidental or deliberate (malicious) modification at any time during transmission or storage. EVIDENCE.com ensures that 100% data integrity is maintained as evidence is passed from the physical AXON devices to EVIDENCE.com via the ETM interfaces using hashing and other methods. Similarly integrity of stored evidence is maintained at all times.

**Availability:** Systems remain available for legitimate users on a 24X7 basis. Regularly scheduled maintenance procedures are performed during low traffic times.

**TASER ensures the integrity of data on EVIDENCE.com by:**

* Encrypting all data transfer between devices (AXON to ETM and ETM to EVIDENCE.com).
* Validating that the entire data has been fully and accurately ingested from AXON to ETM to EVIDENCE.com before informing users to delete it from the ATC.
* Maintaining a full backup of all data at all times in the unlikely event of loss of data or data integrity.
* Performing regular checks on the stored data to ensure there is no loss of data or data integrity.
* TASER personnel get alerts when there are data integrity issues.
* At least two copies of data are kept synchronized all the time.

**Disaster Recovery:** TASER manages all monitoring, alerting and management of data – providing full data visibility and access while keeping your data safe.

**Media Files and Content:** TASER ensures that all data (media files and stored content) on EVIDENCE.com can be recovered in the event of natural or man-made disasters by:

* Leveraging a highly durable storage infrastructure.
* Storing files redundantly on multiple devices across different geographical locations.
* Providing additional protection by using versioning.

**NOTE:** In the event that we do need to recover from unintended user action or application failure, we can restore either the current version or a specified older version. Backups are replicated, which ensures that data is protected in the event of a disaster.

**DATABASE:** TASER ensures that the EVIDENCE.com databases (DB) can be recovered in the event of natural or man-made disasters by:

* In addition to regularly scheduled backups, TASER maintains two copies of DB on different devices.
* To maintain DB high availability, TASER deploys redundant hardware and also replicates the DB data to a standby system.
* For disaster recovery, TASER maintains database backups to an offsite location.