General Security Information

SDFI's multi-layered security framework ensures the SDFI Platform protects your forensic data from capture to sharing.

1. **Overlapping Storyboard Protocol**
   Security begins at the point of image capture. SDFI's Overlapping Storyboard Guideline ensures visual continuity by photographing from a wide view and panning down the body with overlapping images that include consistent anatomical landmarks, reinforcing evidentiary credibility. Areas of interest are documented with mid-range shots, followed by close-ups with and without a forensic scale for clear, verifiable context.

2. **Non-Destructive Image Format**
   Images are captured in the RAW format, a non-destructive file type that preserves original sensor data without compression or alteration. RAW files cannot be overwritten or easily manipulated, making them a reliable format for digital evidence. This ensures that any tampering would be detectable, supporting admissibility in court.

3. **Strong Data Encryption with Passphrases**
   All forensic files are secured using AES 256-bit encryption, combined with long, user-generated passphrases. This ensures that digital evidence is protected from unauthorized access and tampering throughout its lifecycle.

4. **Independent Secure Storage**
   Encrypted data is stored locally or within your network. The data is encrypted before it reaches storage, restricting access to authorized users with the correct passphrase. To prevent data loss due to system failure or disaster, SDFI recommends that organizations keep a redundant backup, ideally stored offsite. Additionally, all activities are tracked through a detailed audit log.

5. **Secure File Sharing via Nested End-to-End Encryption**
   Share Files are packaged and encrypted, using AES 256-bit encryption and protected with a unique user-generated, One-Time Only Passphrase. The encrypted file is then uploaded via secure SSL/TLS channels to the SDFI File Portal. While temporarily at rest, the data remains encrypted and is stored on self-encrypting drives within a secure, SOC-compliant data center. Neither SDFI nor FilesAnywhere have access to unencrypted forensic data at any time. See more details on SDFI's File Portal Security here.

SDFI does not have possession or access to forensic data. Your organization is solely responsible for the regular backup of your digital data and the physical protection of your data storage devices.

The SDFI Workflow Process

Digital evidence is captured using the SDFI High-Resolution Camera System, which is pre-configured to simultaneously record images in RAW and JPG formats. Examiners follow the Overlapping Storyboard Protocol, capturing a series of overlapping images that maintain anatomical context and visual continuity. All images are saved to a high-capacity SD card inserted into the Camera System.

Following user authentication within the SDFI Software, images are encrypted directly on the SD card, then transferred to a Windows 10/11 computer using the SDFI-supplied USB 3.0 card reader. Files are uniquely renamed and securely moved to a network-protected file location within your IT environment, ideally protected by Active Directory to restrict user access further. SD cards serve only as temporary transfer devices and are regularly erased, formatted, and reused. Encrypted files should also be backed up to a secure external drive or corporate network per your organization's IT policies (network storage is strongly recommended to mitigate risks of hardware failure).

Authorized users can view and analyze images through the SDFI Software, which offers non-destructive zoom, annotation, and contrast enhancement tools. While JPG files are used for examination and reporting, the original RAW files remain untouched and serve as proof of image authenticity. Because RAW files are proprietary to the camera model and cannot be modified, they offer a strong layer of evidentiary protection.

Upon request, a Share File can be created to provide subpoenaed evidence to Authorized Third Parties (e.g. law enforcement, district attorney’s offices, etc.). Each file shared is encrypted with AES-256 encryption and a unique, One-Time Only passphrase. The encrypted file is uploaded via SSL/TLS to a secure, SOC-compliant data center. A download link is sent to the recipient, who must receive the passphrase via separate communication (typically by phone) before decrypting and accessing the contents. Once decrypted, the recipient assumes responsibility for the secure handling of the data.