Digital Evidence Storage Requirements

This is intended as a high-level overview of the requirements for digital evidence storage in a multimedia context. Ratings follow the MoSCoW system of Must, Should, Could and Won't. The requirements are split into two sections, File Handling and Functionality.

Systems must be compliant with the principles in the DSTL NPCC Digital Imaging and Multimedia Procedure v3.0 and Recovery and Acquisition of Video Evidence v3.0 and adhere to the Forensic Science Regulator Act 2021 and Statutory Code.

Ingest

- Any file uploaded to the system must be uniquely identifiable.
- The system must be able to ingest and preserve any file type, whether recognised or not.
- The system must be able to accept .exe files (though not necessarily run them)
- There must be confirmation of successful upload.
    - The system must give notification of failed upload.
- The system must preserve metadata associated with the file on ingest.
    - Including but not limited to time and date information
- The system won't alter the file or filename on either import or export. This must be auditable by industry standard methods such as hashing.
- The system must be capable of preserving file structure, i.e. hierarchy of folders and subfolders including proprietary closed formats, to allow for further forensic analysis.
- The system must allow for ingest from physical media as well as networked sources
- System metadata must be generated for indexing each file on ingest. That metadata:
    - Must include case reference.
    - Must include operator ID.
    - Must include crime type – though this could include none.
    - Must include retention time.
    - Should include distressing/disturbing material marker
    - Should allow user generated data, such as exhibit description, venue etc. Could be free text or drop down
- There should be suitably protected and audited routes for third party uploads
    - This must be configurable depending on source, such as:-
        - registered / trusted
        - unknown
    - This must include the request for native (proprietary) format
    - This should include the question is the system time accurate? yes/no/don't know

Operation

- Must have a folder structure
- All actions on the system must be fully audited, including search terms
    - the audit trail must be viewable and exportable
- There must be suitable virus/malware protection
    - This must be kept active and up to date
- It should be possible to export a chain of custody.

    - This should be readily accessible and easy to export
- At a suitably authorised level it must be possible to delete files
    - Which files were deleted and by whom must be audited
- User access must be controllable by the customer / organisation.
- There must be a disaster recovery strategy
    - This must include preservation of the data in the event of either the storage provider or the software provider ceasing trading.
- There must be a published API allowing other systems to interact.
- Must be compatible with 3rd party crime recording systems.
- System generated metadata must be searchable
- Ingested file metadata should be searchable.
- It must be possible to change crime type.
- It must be possible to change retention time.
- The system must be scalable
- It must be possible to increase capacity of the system in terms of storage space and number of users.
- Infrastructure limits on number of concurrent users must be highlighted.
- It should be possible to create and add department level profiles to the system
- It must be possible to share data with the CPS, and CJS partners
    - It must be possible to onward share links with CJS partners
    - It must be possible for an end user to stream the data as well as download it
    - These onward shares must be subject to the same level of access control as the rest of the system
    - The system must be compliant with MME Design and Development Blueprint v2.2 or its latest iteration available from the CPS
    - Relevant metadata must be displayed with the data
- It should be possible to interact with the system using a standard web browser
- The system could offer enhanced functionality to create compilations/photobooks etc.
    - These tools must be force approved according to FSR guidelines
    - Tools access must be configurable on a role specific basis
- The ability to migrate to new storage infrastructure should be designed in.
- There should be two tiers to the storage:
    - Active cases requiring rapid access.
    - Archive storage with slower access times.

Replay

- The system could offer transcoded copies in a playable format.
    - If this functionality is present transcoded files must be clearly marked as transcoded – with a splash screen – and potentially be of lower quality
- Could offer to replay proprietary format
    - If this functionality is offered, then original file metadata must be accurately preserved and displayed

Export

- The system must be able to export the files in their original format.
    - This must be configurable in terms of recipient/content/time.
- The system must be able to export files in a viewable format.
    - This must be configurable in terms of recipient/content/time.