

What You Need to Know: Protecting and Sharing Body Camera Video

Once body cameras are deployed, departments need to think about how the video footage will be shared and protected. For instance, how will the integrity of video files be protected so they can be used as evidence? A body camera program may have less value if the technology doesn't preserve the integrity of video files so they can be admissible in criminal prosecutions, civil cases and internal investigations.

Other questions to answer:

- Will the video management system (VMS) need to integrate the body camera video files with the department's records management system?
- Does the VMS automate the management tasks for video retention and deletion?
- Does the VMS automatically maintain the video in its native format, and provide a verifiable chain of custody, to ensure its validity as evidence in an investigation?
- How do state public disclosure laws define body camera video and restrictions on release?

CHECKLIST:

- ✓ Review security and control capabilities in the cameras and the VMS.
- ✓ Create policies and procedures for controlling and auditing access to stored video files.
- ✓ Check if the data center complies with the FBI Criminal Justice Information Services Division (CJIS) standards around protection from unauthorized access, changes, copying, deletion and release.
- ✓ Identify needed features for video review and types of redaction, e.g., blurring of selected areas in the image.
- ✓ Evaluate how well the VMS supports the work of responding to requests for video release.
- ✓ Develop a staffing plan as well as policies and procedures for video release. For instance, some departments will never release video without a court order, while others release all video footage.