

Cybersecurity Checklist for Records Units



Ten quick checks for protecting public safety records and Criminal Justice Information (CJI).

☐ Review access rights

Check who can view, export, edit, or administer records systems. Remove access that is no longer needed.

☐ Secure removable media

Use only approved drives and media. Follow agency rules for encryption, transport, storage, and disposal.

☐ Follow least privilege

Give each person only the permissions needed for assigned duties. Limit elevated access.

☐ Protect sensitive records

Check recipients and permissions before sharing CJI, PII, juvenile records, BWC footage, or investigative files.

☐ Use MFA

Use agency-approved multifactor authentication wherever required; never approve an unexpected sign-in prompt.

☐ Lock your workstation

Lock the screen whenever you step away. Keep paper records and devices out of public view.

☐ Protect passwords

Use strong, unique passwords and an approved manager. Never share credentials or reuse a work password elsewhere.

☐ Report problems promptly

Report suspicious messages, lost media, unusual access, and accidental disclosures through agency channels.

☐ Check before clicking

Verify unexpected links, attachments, file shares, invoices, or urgent requests through a trusted channel.

☐ Keep software updated

Follow agency IT instructions for updates. Do not defer approved security patches on managed devices.



The right information. The right people. The right access. The right protection.

Reference: FBI CJIS Security Policy v6.1 (June 2026); CISA Secure Our World. Follow agency policy and your CJIS Systems Agency requirements.