

TITLE 6: CRIMES AND CRIMINAL PROCEDURE
DIVISION 9: CRIMINAL JUSTICE SYSTEM COMPONENTS

§ 9211. Security.

Each criminal justice agency shall adopt operational procedures reasonably designed to:

(a) Ensure the physical security of criminal justice information in its custody and to prevent the unauthorized disclosure of such information;

(b) Ensure that when criminal justice information is stored in an automated system, effective and technologically advanced software and hardware designs are instituted to prevent unauthorized access to such information;

(c) Ensure that communication lines, whether dedicated or shared, over which criminal justice information is transmitted, are operated so as to detect and prevent unauthorized inquiries, record updates, destruction of records or unauthorized access or tampering;

(d) Ensure that agency databases in physical locations and in electronic form are protected from unauthorized access, theft, sabotage, fire, flood, wind, or other natural or manmade disasters, and that adequate backup facilities are available so that, in the event that criminal justice information maintained in such repositories is destroyed or damaged, copies of such information are readily available at a backup site; and

(e) Ensure that personnel security procedures are employed, including appropriate background investigations and that the agency has authority to transfer or remove personnel who are judged to be security threats.

Source: PL 13-53, § 3 (111), modified.

Commission Comment: See the comment to 6 CMC § 9201 regarding PL 13-53.