	Department of Human Services **Online Directives Information System**	**Index:** **Revised:** **Next Review:**	**POL1760** **10/04/2019** **10/04/2021**

SUBJECT: Digital Copiers and Security of Data

POLICY:

The Department of Human Services (DHS) will comply with Georgia Crime Information Center (GCIC) rules and regulations by adhering to all state and federal laws governing the use of Criminal Background Investigations. The DHS Office of the Inspector General (OIG) has the responsibility and authority for the enforcement of these procedures (Criminal Justice Information Services (CJIS) Security Policy, Version 5.2, August 2013).

A. Authority

None

B. References

Criminal Justice Information Services (CJIS) Security Policy Version 5.2, 2013
Georgia Crime and Information Center Policy Manual Rev. 2011

C. Applicability

This policy is applicable to all CJIS operators in OIG Background Investigations Unit.

D. Definitions

- *Terminal Agency Coordinator (TAC):* The person designated by an agency head to serve as a liaison between the agency head and the GCIC for complying with GCIC and NCIC/NLETS Policies, Rules and Regulations (GCIC Council Rule 140-1-.02).
- *Criminal History Record Information:* Records that include direct responses from GCIC and National Crime Information Center (NCIC) received as a result of the submission of electronic fingerprints or GCIC Query Terminal responses

E. Responsibilities

The Office of Inspector General Background Investigations Unit is required to ensure the security of any criminal justice data which is stored in all digital devices such as fax machines and scanners used within the OIG BIU. It is the responsibility of the BIU Special Agent in Charge (or authorized designee) and Terminal Agency Coordinators (TACs) to take the following precautions for devices and equipment used to handle criminal history record information (CHRI).

- Ensure that the equipment is physically located in a secure area,
- Ensure that equipment is separated from non-criminal justice/unsecure

networks.
- Apply management controls to limit access to appropriate personnel and guard against inappropriate remote access,
- Maintain control of the hard drive during routine maintenance,
- Ensure proper disposal of the hard disk drive when the device is being taken out of service.
- Ensure that digital devices are not returned to vendors at lease expiration or sent for surplus until the hard drives have been removed and/or all data is properly purged from the device.

Note: The companies from whom the equipment is leased should provide instructions for purging data from hard drives and/or another device memory. Criminal justice agencies should obtain these guidelines and verify that all data has been removed and/or purged before allowing a digital copy device to leave the secured area.

"*Digital copiers pose a potential security risk for the inadvertent release of criminal justice and/or other sensitive information. Agencies should take proper precautions to ensure secure installation, oversight and proper hard-drive sanitization or destruction. Digital copiers and fax machines are shown to present a risk to Criminal Justice Information (CJI). In a digital copier, and in some fax machines, the scanned documents are converted to a digital file and are temporarily stored in the device until a copy is made. The image of the document may reside in the device until it is overwritten or deleted from the device memory or hard drive. Most digital devices use a hard disk drive to store these scanned document images, the same kind of data storage device found in a PC (personal computer). The biggest concern is that data is accessible*
and can be stolen from the digital device's hard disk drive or other non-volatile memory, either by accessing the device remotely or removing the hard disk drive and extracting the data."

F. History

Policy 1760, last reviewed 10/04/2019

G. Evaluation

The OIG BIU Manager/Supervisor evaluates this policy by:

1. Completing quarterly internal audits to ensure all equipment is being used efficiently and properly.
2. Passing any audit with no findings.