1. PURPOSE

It is the policy of the Mesa Police Department PD Information Technology (PDIT) Unit to configure and implement print devices in such a way as to help prevent the accidental or unlawful dissemination of sensitive law enforcement data.

This policy establishes procedural guidelines for all Mesa Police Department (MPD) members and outside personnel who provide maintenance and support to MPD print devices

2. GENERAL

The Print Devices covered in this policy include, but are not limited to copiers, printers, scanners, facsimile (fax) machines, multi-function scan/print devices, and any scan/print device that can retain residual data with a hard drive or other memory configuration.

2.1 Print Devices

A. Printing technology enables scanning, copying, printing, and faxing documents all from a single print device.
B. In addition, "smart" print devices allow for remote diagnostics, troubleshooting, and general centralized management and support. This advanced functionality comes with security risks.
C. Advanced functions generally require print devices to have hard drives, keep job logs, and maintain historical information for diagnostic purposes; therefore, sensitive law enforcement information could be present on print devices at any given time.

2.2 User Responsibilities

A. All MPD members and outside personnel who provide maintenance and/or support to MPD print devices shall comply with the following:
    1. FBI, CJIS, and ACJIS policies. Refer to Arizona Department of Public Safety (DPS) ACJIS Manual.
    2. MPD policies outlining Information Systems Access and Security such as DPM 1.10.15 Information Systems – Access & Security and DPM 1.10.25 Computer Use Protocols.

2.3 Device Configuration

A. Multi-function print devices used by MPD shall be configured to accomplish the following:
    1. Print jobs shall not be queued on the print device's hard drive.

2. Print jobs shall not be stored on the print device for later printing or reprinting.
3. Only outbound fax capabilities are to be enabled, if required, unless approved otherwise.
4. All multi-function print devices that are capable to do so shall be configured with security settings that allow for confidential printing and release of confidential print jobs by a user-defined security code.
5. PDIT shall modify configuration settings as needed to ensure appropriate security measures are in place.
6. Only PDIT members are allowed to modify global configuration settings for print devices.

2.4 Procedural Controls for Service and Support

A. The following procedural controls are required for any service, maintenance, and support functions:
   1. Print device hard drives shall be given to PDIT to be wiped prior to any vendor, contractor, or reseller taking possession of the drive for service or maintenance purposes or if the print device is replaced or removed from service.
   2. PDIT shall retain defective print device hard drives and destroy them.
   3. PDIT may inspect print device log files at any time to ensure compliance with this order.

B. MPD network access may be required for remote diagnostics, troubleshooting, and general centralized management and support.

C. In compliance with FBI CJIS Security Policy and DPS requirements, only members who have successfully completed a criminal justice background check will have access to the MPD network

REFERENCES

- DPM 1.10.15 Information Systems – Access and Security
- DPM 1.10.25 Computer Use Protocols