1. **Purpose** The purpose of this Standard Operating Procedure (SOP) is to define the guidelines and procedures for the secure and compliant management of locally managed Business Unit (BU) printers. This ensures the confidentiality, integrity, and availability of data processed by these devices, mitigating technology risks in alignment with the MAS Technology Risk Management (TRM) Guidelines. This SOP specifically covers printers that are not under the scope of centralized IT scanning or management systems.
2. **Scope** This SOP applies to all multifunction devices (MFDs) and standalone printers that are procured, deployed, and managed locally by individual Business Units within the organization, and which are not centrally managed by the IT department's scanning or endpoint management solutions.
3. **Roles and Responsibilities**

* **Business Unit (BU) Head:**
  + Overall accountability for compliance with this SOP within the BU.
  + Ensures adequate resources are allocated for printer security and management.
* **BU Printer Administrator / Designated Officer:**
  + Responsible for the day-to-day operation, configuration, security, and maintenance of the BU printer(s).
  + Performs regular compliance checks and ensures adherence to the SOP.
  + Acts as the primary point of contact for printer-related incidents and queries.
* **IT Department (Advisory/Support):**
  + Provides technical guidance and support for complex issues (e.g., network connectivity, advanced security configurations).
  + May assist in vulnerability assessments upon request.

1. **Procedures**
   1. **Acquisition and Initial Setup**

* **4.1.1 Vendor Evaluation:** When acquiring new printers, consider vendors with a strong security track record. (Refer to MAS TRM 5.3 System Acquisition)
* **4.1.2 Security Requirements Definition:** Before purchase, define specific security requirements, including robust access control, data encryption capabilities, and secure communication protocols. (Refer to MAS TRM 5.4 Security-by-Design)
* **4.1.3 Physical Placement:** Place printers in secure, restricted areas where unauthorized access can be prevented. For printers handling sensitive data, ensure they are in visually controlled environments.
* **4.1.4 Network Connection:** Connect printers only to approved and secure network segments. Avoid direct connection to the public internet.
  1. **Secure Configuration and Hardening**
* **4.2.1 Change Default Credentials:** Immediately change all default administrator usernames and passwords to strong, unique passwords. (Refer to MAS TRM 9.3 Strong Password Controls)
* **4.2.2 Set Administrator Password:** Implement a strong, complex administrator password for the printer's web interface (Remote UI) and control panel.
* **4.2.3 Disable Unused Services/Ports:** Disable all unnecessary network services, protocols, and ports (e.g., FTP, IPP, SNMPv1/v2 if SNMPv3 is available).
* **4.2.4 Enable Secure Communication:** Configure the printer to use secure communication protocols (e.g., HTTPS for Remote UI, TLS 1.3 for network communication). Disable HTTP access.
* **4.2.5 IP Address Restriction:** Restrict network access to the printer by allowing communication only from designated IP addresses or trusted subnets using the printer's built-in firewall features. (Refer to MAS TRM 11.3 Network Security)
* **4.2.6 User Access Control:**
  + Implement user authentication (e.g., PINs, department IDs, or local user accounts) on the printer to control who can use it.
  + Configure role-based access to printer functions, restricting sensitive features (e.g., scanning to USB, cloud access) to authorized personnel. (Refer to MAS TRM 9.2 User Access Management)
* **4.2.7 Data Encryption (HDD):** Enable data encryption for the printer's internal hard disk drive (HDD) if available. (Refer to MAS TRM 11.2 Data Security)
* **4.2.8 Secure Data Overwrite/Erase:** Configure automatic secure data overwrite or erase of temporary data (e.g., spooled files, scanned images) after job completion.
* **4.2.9 Verify System at Startup:** Enable any "Verify System at Startup" features to ensure the integrity of the printer's firmware and OS.
  1. **Operational Use**
* **4.3.1 Secure Print Function:** Encourage or enforce the use of "Secure Print" or "Confidential Print" features, requiring users to enter a PIN at the printer to release their jobs.
* **4.3.2 Encrypted PDF for Scanning:** When scanning sensitive documents, utilize the printer's functionality to create encrypted or password-protected PDF files.
* **4.3.3 Original Removal Reminder:** Activate the original removal reminder for scanner/copier functions to prevent sensitive documents from being left on the scanner glass.
* **4.3.4 Authorized Storage Media:** Only use authorized and secure USB drives or other external storage media when connecting to the printer for scanning or printing. (Refer to MAS TRM 11.2 Data Security)
  1. **Maintenance and Patch Management**
* **4.4.1 Firmware Updates:** Regularly check for and apply the latest firmware updates and security patches released by the printer manufacturer. Establish a schedule for these checks (e.g., quarterly). (Refer to MAS TRM 7.3 Patch Management)
* **4.4.2 Configuration Backup:** Periodically back up the printer's secure configuration settings.
* **4.4.3 Inventory Update:** Ensure the printer's entry in the BU's asset inventory is kept up-to-date, including model, serial number, firmware version, and location. (Refer to MAS TRM 3.3 Management of Information Assets)
  1. **Monitoring and Incident Management**
* **4.5.1 Enable Logging:** Configure the printer to enable detailed logging of activities, including print jobs, user logins/logouts, configuration changes, and any security alerts.
* **4.5.2 Log Review:** The BU Printer Administrator / Designated Officer must review printer logs periodically (e.g., weekly) for suspicious activities, unauthorized access attempts, or error messages. (Refer to MAS TRM 12.1 Monitoring and Detection)
* **4.5.3 Incident Reporting:** Any suspected security incidents related to the printer (e.g., unauthorized access, data leakage, malware infection) must be immediately reported to the IT Security Incident Response Team (SIRT) following the organization's incident management procedures. (Refer to MAS TRM 7.4 Incident Management)
  1. **Printer Decommissioning and Disposal**
* **4.6.1 Data Wiping:** Before decommissioning, transferring, or disposing of a printer, ensure all data on its internal storage (HDD, SSD, or flash memory) is securely and irrevocably wiped using a method recommended by the manufacturer or IT department (e.g., multi-pass overwrite). Do not rely on simple factory resets for secure data erasure. (Refer to MAS TRM 11.2 Data Security)
* **4.6.2 Physical Disposal:** Arrange for secure physical disposal of the printer through an approved IT asset disposal vendor.
* **4.6.3 Asset Inventory Update:** Update the BU's asset inventory to reflect the disposal or transfer of the printer.

**5. Compliance and Review**

* **5.1 Annual Compliance Check:** An annual compliance check will be performed by the BU Printer Administrator / Designated Officer (or delegated personnel) against this SOP and the MAS TRM guidelines. This check will verify:
  + Current configuration settings match secure baselines.
  + All firmware/software patches are up-to-date.
  + Log reviews are being performed.
  + Physical security measures are in place.
  + User access is appropriately managed.
  + Any identified deviations are documented and remediated.
  + A report on the compliance status will be submitted to the BU Head and, if required, to the IT Department.

**5.2 SOP Review:** This SOP document will be formally reviewed and updated every **2 to 3 years**, or earlier if there are significant changes in technology, threats, or regulatory requirements. The review will involve relevant stakeholders including the BU Head and IT Department representatives.