SOP: Document Copying, Scanning, and Printing Restrictions

This SOP defines **document copying, scanning, and printing restrictions**, outlining the authorized procedures and limitations to ensure secure handling of sensitive and confidential information. It covers guidelines for acceptable use of office equipment, identification of restricted documents, adherence to data privacy policies, user responsibilities, monitoring and auditing practices, and consequences of policy violations. The purpose is to prevent unauthorized duplication or dissemination of proprietary or sensitive materials and maintain organizational information security.

1. Purpose

To establish clear guidelines and restrictions for copying, scanning, and printing documents to prevent unauthorized disclosure or misuse of sensitive or confidential information.

2. Scope

This SOP applies to all employees, contractors, and third-party personnel who have access to office equipment (e.g., copiers, scanners, and printers) in relation to organizational documents.

3. Definitions

- **Restricted Documents:** Materials identified as proprietary, confidential, or subject to data privacy regulations.
- **Authorized User:** An individual with explicit permission to use office equipment for business purposes.

4. Responsibilities

- All users must adhere to this SOP and report any violations or suspicions of misuse.
- IT and Security teams are responsible for monitoring device usage and auditing activities.
- Supervisors are responsible for ensuring their teams understand and comply with these restrictions.

5. Authorized Procedures

1. Only authorized users may access office copiers, scanners, and printers.
2. Before duplicating any document, users must verify if the material is classified as restricted.
3. Copying, scanning, or printing restricted documents is allowed only for legitimate business needs with proper authorization.
4. When handling confidential documents, ensure:
   - Physical and digital copies are safeguarded at all times.
   - Output trays are cleared immediately after use to prevent unauthorized access.
   - Electronic files are sent only to authorized recipients via secure methods.

6. Identification of Restricted Documents

1. Labels or watermarks should be used to visibly identify restricted materials.
2. Consult the Data Classification Policy or direct supervisor if unsure whether a document is restricted.

7. Acceptable Use Guidelines

- Use office equipment solely for work-related tasks.
- Do not use devices to duplicate personal, non-work, or unapproved materials.
- Dispose of unneeded printed or copied sensitive documents using approved shredding or destruction methods.

8. Monitoring and Auditing

1. All device use may be monitored and logged for security and compliance.
2. Routine audits will be performed to detect and investigate irregular activities.

9. Policy Violations and Consequences

- Any violations of this SOP may result in disciplinary action up to and including termination of employment and/or legal action.

- Incidents must be reported immediately to the Security or Compliance Officer.

10. Review and Revision

This SOP will be reviewed annually or as necessary to ensure effectiveness and compliance with regulatory requirements.

Note: Always refer to the latest company data privacy and security policies for further information.