DocuPanda Secure Disposal and Asset Removal Policy

Purpose

This policy establishes the strict requirements for the secure destruction and disposal of paper documents, physical devices, and other media assets within DocuPanda. It aims to ensure that sensitive information, including but not limited to user data, is irreversibly destroyed to prevent unauthorized access or misuse.

Scope

This policy applies to all employees, contractors, and third-party vendors handling any DocuPanda assets. This includes but is not limited to:

- Paper documents
- Physical devices (e.g., laptops, desktops, servers, hard drives, USB drives)
- Electronic media (e.g., DVDs, CDs, backup tapes)

Policy Statement

1. No Storage of User Data on Local Devices

DocuPanda's operational protocols strictly prohibit the storage of user data on any local devices. All user data must be stored exclusively in approved cloud storage solutions: S3, Azure Bucket, and DocumentDB. Any deviation from this protocol constitutes a severe violation of company policy.

2. Authorized Data Disposal

While user data is not stored on devices under normal operations, any physical or digital media that may contain residual data (e.g., temporary files, logs) must be handled with utmost caution.

2.1 Paper Documents

- **Classification**: All paper documents are classified as confidential by default.
- **Destruction**: Shred using a cross-cut shredder. If outsourced, use only DocuPanda-approved third-party shredding services.
- **Verification**: Destruction must be verified by a supervisor or authorized personnel.

2.2 Physical Devices

- **Data Wiping**: Before disposal or repurposing, all physical devices must undergo data wiping using DocuPanda's approved software tools (e.g., DoD 5220.22-M standard).
- **Destruction**: For devices that cannot be wiped, physical destruction is mandatory:
  - Hard drives must be degaussed and shredded.
  - Solid-state drives (SSDs) must be physically shredded.
  - Mobile devices must be factory reset and then destroyed if applicable.
- **Documentation**: The destruction process must be documented and signed off by authorized personnel.

2.3 Electronic Media

- **Destruction**: All electronic media (DVDs, CDs, tapes) must be shredded or pulverized.
- **Verification**: Destruction must be performed under supervision and documented.

3. Third-Party Disposal Services

When using third-party disposal services: - Ensure the vendor complies with DocuPanda's security standards. - Obtain a certificate of destruction for all destroyed assets. - Conduct periodic audits of third-party service providers.

4. Training and Awareness

All employees and contractors must: - Complete annual training on secure disposal and destruction procedures. - Sign an acknowledgment form confirming understanding and compliance with this policy.

5. Compliance and Penalties

Failure to comply with this policy will result in disciplinary action, up to and including termination of employment or contract. Legal action may be pursued in cases of gross negligence or willful misconduct.

Procedure for Reporting

Any suspected or actual deviation from this policy must be reported immediately to the Security Team via [internal reporting tool or contact method].

Review and Updates

This policy will be reviewed annually or as required by changes in legal, regulatory, or business requirements. Updates will be communicated to all relevant parties.

Approved by: Uri Merhav (CIO)
Policy Owner: Security Team
Effective Date: 10/01/2024
Next Review Date: 01/01/2025