Security Overview

Encryption Method

- AES (Advanced Encryption Standard) is used to encrypt all files before saving.
- Ensures files remain unreadable without the key.
- Decryption occurs only during download.

Key Management

- AES key stored in .env outside the codebase.
- Loaded at runtime using python-dotenv.
- Never committed to GitHub.

File Handling

- Files are encrypted immediately upon upload; plaintext is never stored.
- Decrypted on-the-fly during download.
- uploads/ folder stores only encrypted .enc files.

Secure Deletion

- Delete uses POST requests to prevent accidental deletion.
- User confirmation required.
- Deleted files are permanently removed.

Additional Security Considerations

- Optional file integrity checks (SHA256) for verification.
- Flash messages provide user feedback.
- No sensitive information exposed in UI or logs.

Summary

- Ensures **confidentiality**, **integrity**, and **controlled file access** via AES encryption, secure key management, and safe file handling.