Secure GED Workflow – Zero Trust & Defense in Depth (v2)

This document describes a hardened, implementation-ready security workflow for a Document Management System (GED). The design follows Zero Trust principles, Defense in Depth, and audit-grade security controls.

1. Identity, Access & Session Establishment

- User authentication via identifier + password
- Mandatory MFA (TOTP, hardware key, or push)
- Progressive anti-bruteforce protection (rate limiting, CAPTCHA, alerts)
- Session ID regeneration after authentication and privilege changes
- Hardened cookies (HttpOnly, Secure, SameSite=Strict)
- Context evaluation (IP reputation, device fingerprint, anomaly detection)

2. Secure File Ingestion & Quarantine

- Uploaded files are treated as untrusted by default
- Initial placement in isolated memory or quarantine zone
- Enforced file size limits and decompression guards
- Binary signature validation (magic numbers)
- Filename and path sanitization
- Antivirus and malware scanning (external engine)
- Optional content sanitization (PDF scripts, macros)
- SHA-256 hash generation for integrity tracking
- Immediate rejection and alert on any validation failure

3. Secure Storage & Cryptography (Data at Rest)

- Document encryption using AES-256 before persistence
- Metadata encryption for sensitive attributes
- Envelope encryption with external KMS / Vault
- Strict key isolation from encrypted data
- Key rotation and revocation policies
- Encrypted, access-controlled backups

4. Authorization & Policy Enforcement

- Deny-by-default access model
- Object-Level Permissions (OLP)
- Access decision based on user clearance and document classification
- Least privilege enforcement
- Optional contextual constraints (time, location, action type)

5. Secure Retrieval & Protected View

- No direct file URLs exposed
- Access through authenticated proxy endpoints
- Final authorization check at view time

- Decryption performed only in volatile memory (RAM)
- Secure HTTP streaming to client
- Mandatory watermarking for sensitive classifications
- Explicit acknowledgment of client-side leakage limits

6. Audit, Traceability & Non-Repudiation

- Comprehensive event logging (auth, access, changes)
- Append-only or WORM log storage
- Cryptographic log integrity (hash chaining or signing)
- Trusted time source for timestamps
- Restricted and monitored log access
- Optional PKI-based document signatures

Conclusion

This workflow provides a vault-grade GED security architecture. It balances strong cryptographic controls, continuous verification, and operational realism while maintaining clear scope boundaries.