Encrypted Document

EDITION	CAPABILITY	SIGNATURE	STANDARDS	GENERATED
Core	AES-256 encryption	Not signed · encrypted	ISO 32000-2	2026-08-17

This document is **AES-256 encrypted**; it opens without a password for this demonstration; copy and modify permissions are set and enforced by conforming readers. Every string and stream in the file — page content, fonts, metadata values — is stored as AES-256 ciphertext; what you are reading now was decrypted by your viewer using the file's own encryption dictionary.

WHY IT MATTERS

Encryption at the file level travels with the document: the same protections apply from email attachment to archive to print queue, with no server in the loop. An empty user password keeps the reading experience frictionless while the owner password and the permission flags still gate copying, extraction, and modification in conforming readers.

ENCRYPTION

Handler	Standard (/Filter)
Algorithm	AES-256 · V5 / R6 / AESV3
Mode	CBC, random IV
Key length	256-bit
User password	empty — opens freely
Owner password	demo-owner-key-2026

Permission matrix

The /P bitmask below is written into the encryption dictionary and sealed into the AES-encrypted /Perms value, so tampering with the flags is detectable. Bits follow ISO 32000-2:2020, Table 22.

Permission	Table 22 bit	This document
Print the document	3	Allowed
Modify contents	4	**Denied**
Copy / extract text and graphics	5	**Denied**
Add or modify annotations	6	Allowed
Fill in form fields	9	Allowed
Extract for accessibility	10	Allowed
Assemble the document	11	Allowed
High-resolution printing	12	Allowed

How the protection works

1. **Key derivation.** The 256-bit file encryption key is derived from the passwords with the hardened SHA-2 based hash of ISO 32000-2 §7.6.4.3.4 (revision 6), then stored AES-wrapped in the /U and /O key material — the file key itself never appears in the file.
2. **Content encryption.** Both crypt filters (/StmF and /StrF) use /AESV3: each string and stream is encrypted with AES-256 in CBC mode under a fresh random IV, which is why an encrypted PDF is intentionally not byte-reproducible.
3. **Permission enforcement.** The /P flags are duplicated into the AES-ECB-sealed /Perms entry, so a conforming reader can verify the declared permissions cryptographically before honoring them.

The owner password above is published on purpose — this file is a public capability demonstration and protects nothing sensitive. In production, keep the owner password secret and empty the user password only when the document should open without a prompt.