PDF security and redaction checklist.

Most document leaks are simple mistakes: a black box that was not real redaction, a forgotten comment, or the wrong attachment. Run this checklist before a private PDF leaves your office.

BEFORE YOU SEND

Check the content.

Look at what is actually in the file.

- [ ] Is this the right file and the right version?
- [ ] Remove pages the reader does not need.
- [ ] Delete comments and notes meant only for your team.
- [ ] Check headers, footers and watermarks.

REDACTION

Remove private details for real.

Covering is not removing.

- [ ] Use a real redaction tool, not black boxes or highlighter.
- [ ] Redact names, account numbers, tax IDs and signatures as needed.
- [ ] Search the saved file for a redacted word. Nothing should come back.
- [ ] Keep the unredacted original somewhere secure.

PROTECTION

Lock what needs locking.

Match protection to how private the file is.

- [ ] Add a password to files with private data.
- [ ] Limit printing, copying or editing if needed.
- [ ] Send the password a different way than the file.
- [ ] Add a CONFIDENTIAL watermark as a reminder.

SHARING

Share it safely.

The last step is where most mistakes happen.

- [ ] Double-check the recipient email address.

- [ ] Share a link from SharePoint or OneDrive instead of attaching when you can.
- [ ] Do not upload private files to unapproved websites.
- [ ] Only use AI tools your company approved.