CUSTOM SOFTWARE

Before Designing Screens, Decide Who Can Change What

The application works in the demonstration because the presenter can do everything. Problems appear when the team starts using it: someone needs to prepare an order but can also change its price, delete the record and export every customer.

Describe Tasks as Well as Job Titles

A list of job titles does not explain every permission. Two people with the same title may work in different branches. Start with concrete tasks: viewing, creating, correcting, approving, exporting or deleting. Decide which records each person can act on and when a second approval is needed.

Turn those decisions into examples. An operator might correct an address before dispatch, while a later change should become a recorded exception. The rule depends on the actual process and should be explainable without reading code.

Hiding a Button Is Not Enough

The system must check permissions where it processes an operation, even when the screen hides the action. During testing, attempt a task with an account that lacks permission and confirm it is rejected without changing data. Repeat with another branch’s or customer’s records wherever that separation exists.

- Verify what each role can do and what must remain outside its reach.
- Record relevant changes with an author and time, without storing secrets in the history.
- Define how temporary access is granted and who removes it.
- Include an explanation of permissions and a way to review them in the handover.

A permission that blocks everyday work tends to produce shared passwords or requests to make everyone an administrator. Test the rules with the people doing the work and repair the process before falling back on that workaround.

Permissions limit what an account can do inside the system. They need testing and maintenance and do not replace device protection or control over administrator accounts.

A Check You Can Run

Write one permission as a testable sentence: a salesperson may draft a refund request for their own customer but may not approve it. In an authorised test environment, check the permitted action, the forbidden approval and access to another customer’s request. Include export and bulk actions in the same review, since a restricted screen can still have another route to the data.

Supporting guidance: OWASP’s authorisation checklist.
https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html

Continue with: When Someone Leaves, Which Access Stays?.
https://systems.kavaliero.com/en/blog/when-someone-leaves-which-access-stays

For help with this work, see the scope of Custom Software.
https://systems.kavaliero.com/en/services/custom-software