

Share information and access safely

What to prepare now, and what to share only after the project process is agreed.

🕒 4 min read Updated October 2026

Start with descriptions and safe examples

For early discussions, describe your data and tools without sending the data itself. Use anonymised examples that remove names, phone numbers, addresses, payment details, and other identifiers. A systems list is usually enough to begin scoping.

Agree access deliberately

- Name the account owner and the person allowed to approve access.
- Use named invitations and limited roles where the platform supports them.
- Agree a secure route for secrets if they are required. Never put passwords or API keys in a public form or shared brief.
- Confirm testing, production access, and who removes or changes access at handover.

Define the data boundary

Before using confidential information, agree the relevant confidentiality terms, data roles, providers, hosting location where required, retention, deletion, and access controls. The right setup depends on the service and contract. Public guides are not evidence of a particular certification or deployment arrangement.

Your checklist

0/4 complete

- ☐ Prepare an account and systems inventory.
- ☐ Remove identifiers from examples.
- ☐ Name access approvers.
- ☐ List data restrictions before scoping.

A USEFUL NEXT STEP

Discuss your requirements before sharing sensitive files or granting access.

Your signed proposal and agreement define the final scope, fees, responsibilities, and terms.

resources.swepety.com · support@swepety.com