NamoID

Pre-Demo-Day Security Checklist

A practical review for startup teams, incubators, accelerators, and university innovation cells. Use synthetic data only. This checklist is product guidance, not legal advice, certification, or a penetration test.

Startup		**Review date**	
Reviewer		**Demo date**	

1. Separate the demo from production

[ ]	The demo uses a dedicated Test or sandbox environment.
[ ]	All accounts and profiles are synthetic and clearly labelled.
[ ]	No real Aadhaar, PAN, DigiLocker, KYC, payment, health, or customer documents appear.
[ ]	Secrets are stored outside source code, screenshots, and presentation files.
[ ]	The repository contains no committed environment file, token, private key, or database export.
[ ]	The demo can be reset without affecting production users.

2. Check login and account creation

[ ]	The product does not ship with a shared default password.
[ ]	Passwords are handled by an appropriate authentication system and never stored in plain text.
[ ]	Verification and one-time-password requests have abuse controls.
[ ]	Public responses do not reveal whether a sensitive account exists unnecessarily.
[ ]	Redirect and callback URLs are restricted to intended destinations.
[ ]	Test administrator accounts use credentials distinct from participant accounts.

3. Review administrator access

[ ]	Every administrator has an individual account.
[ ]	Privileged access is limited to people who need it.
[ ]	The team can remove access when a member leaves.
[ ]	Sensitive administrative actions use recent or stronger authentication where appropriate.
[ ]	Important changes create an audit event with actor, action, target, and time.
[ ]	Administrative routes are protected by authorization, not only hidden navigation.

4. Test account recovery

- [ ] The team has documented what happens when a password, passkey, email, or phone is lost.
- [ ] Recovery does not rely only on profile facts an attacker could discover.
- [ ] Recovery links or codes expire and cannot be reused indefinitely.
- [ ] Successful recovery invalidates access that should no longer remain active.
- [ ] Users receive a clear notification when important recovery details change.
- [ ] Support cannot bypass recovery controls without an accountable process.

5. Minimize personal data

- [ ] Every signup field has a current, documented purpose.
- [ ] Optional fields are visibly optional.
- [ ] The product explains why sensitive data is requested.
- [ ] The team knows which processors receive personal data.
- [ ] Users can find the relevant correction, deletion, or support path.
- [ ] Logs and analytics do not capture passwords, tokens, one-time codes, or identity documents.

6. Prepare the failure path

- [ ] The demo shows what happens when authentication fails.
- [ ] Rate limits and upstream failures produce a usable response.
- [ ] The team can revoke a session or disable a compromised account.
- [ ] A named person owns incident triage during the demo.
- [ ] The team knows how to contact each critical provider.
- [ ] The presentation distinguishes working, mocked, and planned features.

Readiness result

GREEN	Checked and tested.
AMBER	Known limitation with an owner and deadline.
RED	Could expose credentials, personal data, privileged access, or production users. Fix before the demo.

Complete guide: namoid.in/blog/demo-day-security-checklist-startups
Incubator partnerships: namoid.in/blog/namoid-incubator-accelerator-partnerships
Community and setup help: join.slack.com/t/namoidcommunity