

Orb Labs AG — Confidentiality & Security

Confidentiality & Security

Our clients share sensitive material with us — data rooms, cap tables, term sheets, and internal documents. Protecting that material is fundamental to how we work. This page explains the commitments and controls behind every engagement.

Our confidentiality commitments

- **Every engagement is under NDA.** We work under your NDA, ours, or a mutual form as agreed. We expect to sign before any material changes hands.
 - **Used only for your engagement.** Material you share is used solely to produce your report. It is never used for any other client, purpose, or our own activities.
 - **Never redistributed.** We do not share, sell, or disclose your materials to third parties, except where strictly required by law — and where lawful, we would notify you first.
 - **Bound team.** Anyone with access to your material is bound by written confidentiality obligations.
-

How we handle your materials

We keep a deliberately small footprint for client data — the less that is held, and the fewer who can reach it, the safer it is.

1. **Receipt.** Materials are received through a secure channel — [your secure data room / encrypted file transfer, e.g. provider name] — not ordinary email attachments.
 2. **Access.** Access is limited to the individuals working on your engagement, on a least-privilege basis. [Number of people, typically very few.]
 3. **Storage.** Materials are stored in [access-controlled, encrypted storage — name the system], not copied to personal or unmanaged devices.
 4. **Return or deletion.** On completion, we return or securely delete your materials within [10 business days], retaining only the minimum records we are legally required to keep (see Retention).
-

Information security controls

NOTE: list only what you actually do. The items below are a realistic baseline for a boutique; adjust to your stack.

- **Encryption** of data in transit, and at rest where supported by our storage and transfer tools.
- **Access control** with strong authentication, including multi-factor authentication on accounts that touch client data.
- **Least privilege** — access granted only as needed and removed when no longer needed.
- **Device security** — [managed devices / disk encryption / screen lock / up-to-date systems].
- **Vendor diligence** — we use reputable providers and rely on their security and compliance posture (see Subprocessors).
- **No public exposure** — client materials are never placed on public links, shared drives, or unsecured locations.

We do not currently hold [ISO 27001 / SOC 2] certification.

Subprocessors and tools

We rely on a small set of trusted providers for secure file exchange, storage, and communication. We require each to maintain appropriate security and to process data only on our instructions. Some may be located outside Switzerland; international transfers are handled as described in our Privacy Policy.

Separation from our own activities

Our founder is an active investor. Client materials are walled off from that activity: confidential information you share is never used to inform our own or anyone else's investment decisions. This separation, together with our Conflict-of-Interest & Independence Policy, is part of how we keep our research independent and your information safe.

Retention and deletion

We hold client materials only for as long as the engagement requires. After delivery, materials are returned or securely deleted within [10 business days]. We retain a minimal engagement record (e.g., scope, invoice, final report) for [period / legal retention] by Swiss law, stored under the same controls. Details are set out in our Privacy Policy.

If something goes wrong

No system is perfectly secure. If a security incident affected your materials, we would investigate promptly, take steps to contain and remediate it, and notify you without undue delay, along with any authority notification required by law.

What we ask of you

To keep material safe on both sides:

- Share documents only through the secure channel we provide.
 - Send the minimum necessary — redact what isn't needed for the analysis.
 - Flag anything especially sensitive so we can handle it accordingly.
-

Questions

We're glad to walk your operations or compliance team through our practices and to provide our NDA or a short security summary on request.
