

Customer NDA

Confidentiality should protect both parties without obstructing lawful audit, security response or necessary delivery.

01 / Protected information

A mutual NDA should cover information identified as confidential or reasonably understood to be confidential, including architecture, pricing, vulnerabilities and business plans. It should exclude information already public, independently developed or lawfully received without restriction.

02 / Permitted disclosure

Use is limited to the stated business purpose. Disclosure is on a need-to-know basis to bound personnel and advisers; compelled disclosure is handled with notice where lawful. Security safeguards should reflect the sensitivity of the information.

03 / Duration and data

The executed NDA specifies term, survival, return or destruction, remedies and governing law. Personal-data processing on behalf of a controller requires a separate GDPR-compliant processing agreement when applicable.

Document status

Original VISIONCYBERX working framework for review. This PDF is not an offer, a signed agreement or evidence of an implemented control. Confirm legal entity details, service scope, commercial terms, annexes and approval before use. A signed engagement document governs.

Official EU references

GDPR, Article 28