

Code of Conduct

Business-first security requires integrity in the advice, data handling and relationships behind every recommendation.

01 / Professional conduct

Act lawfully and honestly, describe limitations, avoid misleading certification claims and distinguish a vendor's obligations from our own. Declare material conflicts and do not let undisclosed incentives determine a shortlist.

02 / Protect information

Apply least-privilege access and the customer's agreed security rules. Share confidential material only for the authorised purpose and escalate a suspected incident without delay through the agreed channel.

03 / Decisions and concerns

Document significant assumptions, approvals and risk acceptance. Raise suspected misconduct through the relevant manager or Projects@visioncyberx.com. The signed engagement and any internal policy govern investigation and remedies.

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 32

NIS2 Directive, Article 21