dcodx B.V.
Ceramiquelaan 563
Amsterdam, 1031KG
info@dcodx.com - dcodx.com

Security Programs Terms and Conditions

1. Program Scope

The DCODX Application Security Program includes penetration testing, developer training, and application security advisory services as defined in the selected package (SME, Growth, Enterprise).

Services are delivered remotely unless otherwise agreed.

2. Advisory Hours Usage

The program includes a predefined number of advisory hours per year depending on the selected package.

Advisory hours may be used for:

- Vulnerability remediation support
- Architecture and security design discussions
- DevSecOps guidance
- Threat modeling sessions
- Security roadmap reviews
- Awerenss sessions on latest threats
- Workshops

Unused hours do not roll over unless agreed otherwise.

Additional hours can be purchased at DCODX standard consulting rates.

3. Pentest Scope

The program includes the number of pentests specified in the selected package.

Each pentest covers a predefined scope agreed before the assessment and may include:

- Web applications
- APIs
- Mobile applications
- AI integrations
- Network

Large scope changes may require additional effort to be agreed upon.

4. Retest Conditions

Retests are limited to validating vulnerabilities identified during the original pentest.

New features introduced after the initial assessment may require additional testing and avisory hours could be used for that.

5. Secure Coding Training

Training sessions are delivered remotely unless otherwise agreed and include hands-on labs and practical demonstrations. The number of participants should be agreed in advance.

Additional participants may require additional licenses or fees.

6. Scheduling

Pentests, training sessions, and advisory meetings must be scheduled in advance and are subject to availability.

Clients are encouraged to plan pentests and training at least 4 to 6 weeks in advance

7. Client Responsibilities

The client must provide:

- access to applications or environments
- access to the code if required
- Communication channel
- necessary documentation
- testing credentials when required
- a point of contact during assessments

8. Confidentiality

All information obtained during the engagement will be treated as confidential and will not be disclosed without prior consent.

9. Limitations

The program does not guarantee the identification of all vulnerabilities or the prevention of security incidents.

Security assessments are point-in-time evaluations.

Advisory hours can be used to setup continuous security automation as part of the development cycle.

10. Program Duration

The Application Security Program is structured as a yearly engagement.

Services must be used within the contract period unless otherwise agreed.

11. Change of Scope

Significant changes to the application architecture or scope may require adjustments to the engagement.

12. Cancellation / Rescheduling

Training sessions and pentests may be rescheduled with at least 10 business days notice.