



Running a Security Program

Last updated on August 1, 2026

IMPORTANT - READ BEFORE USING THE SITE OR SERVICES FOR RUNNING A SECURITY PROGRAM.

These Running a Security Program terms ("**Supplemental Terms**") form a part of the Platform Services Agreement or other similar agreement between Customer and Cobalt ("Agreement") and you, as an authorized agent of the entity who has executed a Sales Order or other similar purchasing document with Cobalt ("Customer"), agree that you are a User of the Platform and Services, and Customer has already agreed to and accepted the Agreement and Privacy Policy and you are an authorized User on the Platform. Terms not otherwise defined herein, shall have the meaning set forth in the Agreement.

Security Program Time Period

The Security Program initiates when it is listed on the Platform and has the status Live.

The Security Program will run until a written deadline agreed between Customer and Cobalt. This deadline will be listed on the Security Program.

Security Professionals can only engage in testing on programs that are in status Live and the Security Professionals have been assigned. When a program is past the test deadline, Security Professionals are not allowed to engage in test activities other than re-testing / Patch verification specifically requested by Customer.

The date on which your test will start may depend on the Tier associated with your account. Each Tier permits test start dates within a defined minimum advance notice, measured in Business Days ("**Minimum Notice Period**"). For purposes of calculating the applicable period associated with your Tier, a "**Business Day**" falls within Cobalt Business Hours and excludes holidays and weekends, provided that a test must be assigned a test to "**Planned**" prior to 11 AM Pacific Standard Time of the first day of the Minimum Notice Period. "**Cobalt Business Hours**" are: for customers in EMEA, 8 AM - 5 PM Central European Standard Time; for customers in the Americas, 8 AM Eastern Time- 5 PM Pacific Time. Cobalt's commitment to initiate a test within a certain period only begins when a test is listed as "**Planned**" and a start date is selected. Services must be scheduled to be completed within the applicable annualized period of the applicable Service Period on a Sales Order. When Services that are scheduled to begin within thirty (30) days of the expiration of the one-year period associated with the applicable Credit(s), test coverage may be reduced, and retesting may be precluded due to time and resource constraints.

Third-party Integrations

Services may be configured to facilitate integration with certain third-party software products or services leveraged by Cobalt customers. The availability of such integrations is dependent on the specific Tier assigned to a Customer.

Notwithstanding the foregoing, Cobalt reserves the right to deprecate any particular third-party integration at its discretion.

By accessing or using Cobalt's third-party integrations, Customer represents and warrants that it has obtained all necessary licenses, credentials, or other rights to facilitate Customer leveraging such third-party integrations.

Cobalt hereby disclaims any and all obligations relative to such third-party's privacy or security posture.

Customer uses such third-party integrations at its own risk. Cobalt does not make any warranty for and shall not be held liable or accept any liability, obligation, or responsibility for any loss or damage in connection with any third-party integration. Cobalt has no control over such third-parties and Cobalt is not responsible for the content of their services. Cobalt provides Customer with third-party integrations only Customer's convenience.

Services Timing

All testing must be completed during the applicable annual Service Period. Request Services at least 30 days prior to the end of the annual Service Period. Standard testing period for Platform Services (excluding autonomous testing) is 14 days.

Retesting

Cobalt may offer retesting of vulnerabilities, depending on the Tier you purchased, as further described in Cobalt's [Tiers FAQ](#). Retesting consists of Security Professionals re-engaging via the same or similar methodologies in testing of specified vulnerabilities that were originally identified in a Vulnerability Report. Retesting is applicable only to those vulnerabilities that you have taken steps to remediate, and the intent of retesting is to validate the efficacy of your remediation efforts. Timing for retesting is at Cobalt's sole discretion. Customer cooperation with Cobalt operational requests (including without limitation, providing access to credentials and environments) is a condition to Cobalt's retesting obligations. Customer must request a retest by at least ten (10) days prior to the expiration of their Services Period (unless Customer has executed a renewal). Retesting is subject to all terms and conditions otherwise applicable to the provision of Services by Cobalt.

Security Program Responsibilities and Liabilities

- Customer authorizes Cobalt to list your program on the Platform.
- Customer authorized invited Security Professionals to perform tests on the Application(s)/Network(s) mentioned in scope in the Security Program.
- Customer agrees to take the full liability and responsibility, and release Cobalt from any liability, if Customer allows anyone who is not a Security Professional or other non-Cobalt personnel, is engaged in testing of the Security Program.
- Customer agrees that the scope, rules and all other information on the Security Program is the entire scope, rules and information which you expect the Security Professionals to follow if engaging in activities related to your Security Program.
- Customer agrees that Cobalt only provides a best practice set of rules as an example and that Customer's User is fully responsible and liable for the coverage of the scope and the rules written in the Security Program.
- Customer agrees that you are responsible for contacting and getting, if needed, acceptance from any and all related third parties who potentially will be impacted by the activities related to the Security Program. This includes but is not limited to hosting providers.
- You agree that you understand when you initiate the Security Program you will start receiving Vulnerability Reports on the Platform. This means that Cobalt will store these Vulnerability Reports on the Platform, any vulnerability/bug submitted against Customer's Security Program will only be visible to Customer's Users, the Security Professionals participating in the Security Program and authorized staff at Cobalt.
- In the event Customer's Security Program has responsible disclosure Customer agrees that Customer is responsible for informing the Security Professionals on when he/she can disclose a given vulnerability to the public. No such disclosure will be made by the Security Professionals if not authorized by Customer.

Privacy

User agrees and acknowledges that the personal data User provides to Cobalt may be processed for the purpose of providing the Services. Each Party shall maintain appropriate technical and organizational safeguards for protection of the associated personal data that is collected and/or processed through User's use of the Services.

For more information on Cobalt's data privacy practices, please see our [Privacy Policy](#) or contact us at privacy@cobalt.io.

Any false information provided within the context of the Security Program by Customer concerning identity, mailing address, telephone number, email address, ownership of right or non-compliance with these terms and conditions or the like may result in the immediate termination of the Security Program.

Insurance/Backup

Cobalt recommends that Customer obtains appropriate insurance and backup for Assets and its content. Please review any insurance policy for the Assets and its content carefully, and in particular please make sure that yCustomer is familiar with and understand any exclusions to, and any deductibles that may apply for, such insurance policy.

Complete Agreement and Order of Precedence

All of the terms set forth in the Agreement shall apply to these Supplemental Terms including without limitation confidentiality, liability, controlling law and jurisdiction, dispute resolution and arbitration and costs. In the event of a conflict between the Agreement, and these Supplemental Terms, the Supplemental Terms shall apply.