

Legal

We connect companies with ethical hackers, by means of our crowd-sourced security platform. Before reviewing our services and agreements, your legal, privacy or procurement department may be interested to learn more about how we offer our services from a contractual perspective.



Which services do we offer?

To understand our contracts, it is important to understand the scope of our services. We offer 2 main service components:



Scope of Services

By means of our **Crowd-Sourced Security Platform**, we connect your company with a community of over **90,000 independent ethical hackers** (aka "Researchers"). Our platform is fully managed and provides specific functionalities for collaboration in respect of Vulnerability Disclosure Programs and other security testing services.

Ancillary Services

In **addition to our SaaS platform**, we offer several ancillary services, such as onboarding, assistance with shaping your (bug bounty) program, triage of reported vulnerabilities, Researcher ID Verification and screening, community management, bounty payments, and dispute assistance.

Summarized: We are here to help.



What makes up the contracting framework?

1. MSA

Our **Master Services Agreement** ("MSA") governs the relationship between Intigriti and your company. The MSA explains **your rights in respect of the platform**, how you can **collaborate with Researchers**, and **sets out our respective roles and responsibilities**.

2. Researcher T&Cs

The Researcher terms and conditions set out the base rules that Researchers must comply with when working on your (bug bounty) programs.

3. Data Schedule

Our **Data Schedule** describes how we handle the data you upload onto our platform. You will mainly use our platform to **publish** (bug bounty) **programs and store your submissions**. As these are not personal data, our Data Schedule handles more than PII alone.

4. Program Conditions

You are **in control of your program** and can determine what a Researcher is or is not allowed to do when participating in your program. In your Program Conditions, you can describe the **scope, access restrictions, bounties, and any do's or don'ts**.

Your Program Conditions take precedence over the Research T&C.



Consult the Researcher T&C at:
go.intigriti.com/tac



Intigriti Legal FAQ

Why are researchers not our subcontractors?

Our collaboration platform facilitates continuous vulnerability testing with the assistance of an extensive community of independent security researchers, each bringing their own unique experience and expertise to the table. This cannot be achieved with a traditional pentesting approach. Moreover, your company is in control of its programs and can freely determine the testing scope, testing timeframe, and which researchers are allowed to

participate in your program.

We do not monitor or control your program assignments, and it is up to the researchers to decide whether they are willing to work on your program. We are here to help and facilitate, and to verify the accuracy of reported vulnerabilities, but we do not perform pentests, neither ourselves nor with the assistance of any subcontractors.

Can we use our own MSA?

Intigriti has defined and refined the best possible legal framework to protect and serve its clients. It has crafted an MSA that is fit for purpose and adequately captures the unique aspects of our services provision, including bug bounty and the collaboration relationship with researchers. Clients that use Intigriti's MSA have transitioned through the legal process the quickest and easiest due to the nature

of Intigriti's services, which differ from a typical SaaS or security testing engagement.

Intigriti strongly advises using its MSA, which has been created on the most fair and balanced terms for both your company and Intigriti, with a view to a long-term collaboration.

What kind of data do you process? Is Intigriti a data processor?

You will use our platform to host your (bug bounty) programs and to store and process vulnerability reports submitted by Researchers. As programs and vulnerability reports should not contain personal data, we do not position ourselves as a personal data processor in this context. However, if an asset in scope of your (bug bounty) program does contain personal data and a vulnerability

is reported of such nature and severity, it exposes such personal data. We might become able to access (process) the same exposed data when we triage. We will not download or host such data.

Our Data Schedule explains how we act in this respect and is in compliance with article 28.

TAKE YOUR FIRST STEPS

-  Request a demo www.intigriti.com/demo
-  Visit the website www.intigriti.com
-  Get in touch hello@intigriti.com

