Hacking with permission: the rules that make it ethical

BY ELEANOR BARLOW · MARCH 12, 2026

Ethical hacking, often via Bug Bounty Programs or VDPs, operates within defined frameworks. These include a community Code of Conduct (CoC), setting program Rules of Engagement (RoE), and clarifying platform Terms of Service (ToS). Companies that invest in proactive security need to understand what these terms mean and the function they play in maintaining a secure and compliant program.

The challenge is that security terminologies are often multifaceted, making it demanding for businesses to interpret swiftly and effectively.

It should be noted that **this blog does not constitute legal advice**, but serves to educate and explain these concepts, to remove legalese, and directly highlight the business impact.

What does a Code of Conduct (CoC) mean in ethical hacking?

The Code of Conduct is, in essence, what separates ethical hackers from malicious threat actors, and stands as the guiding light of most Bug Bounty programs and other proactive forms of security testing.

When a researcher is provided with the permissions to investigate and probe for vulnerabilities, this comes with a significant level of responsibility to conduct their testing not only legally, but also professionally.

With a Code of Conduct in place, researchers act with integrity, report responsibly, protect information they encounter, actively avoid causing any disruption or damage, and **only test what they are authorized to test**. It, essentially, provides a set of ethical standards and expectations in terms of how security researchers must execute their activities and defines what ethical means in practice.

What is the business impact of a Code of Conduct?

A well-defined CoC sets expectations and boundaries and reinforces the fact that ethical hacking, especially via a Bug Bounty Program, is a structured security practice.

By setting clear terms, the risk from external testers is reduced. The business agrees on the scope and disclosure practices, and controls what should or should not be tested. Responsibility is clear. Researchers know what is expected of them, which further supports the relationship.

View the Intigriti Code of Conduct for specifics on how Intigriti works with companies to ensure high standards of fair and respectful treatment of individuals, a safe working environment, and other ethical practices.

What's the difference between CoC and Rules of Engagement (RoE) in a Bug Bounty program?

While the Code of Conduct outlines the ethical standards of how both the researcher and company must behave, the Rules of Engagement (RoE) are the backbone of Bug Bounty Programs that highlight operational boundaries of what researchers are allowed to test, to protect infrastructure, and reduce any operational risk.

Rules of Engagement frameworks describe what can be tested, what should be tested, and how these tests should be conducted. They include details about who is eligible for program participation, what contents should be in a report, areas of disinterest, and focus on elements such as setting boundaries to apps, systems, or domains, and specify any expectations, restrictions, or prohibitions that should be put in place.

What is the impact of the Rules of Engagement on business?

The purpose of RoE is to set clear expectations around collaboration. Which means that businesses need to keep rules of engagement focused, clear, and well-structured to ensure that researchers, from any background or language, can understand how to test responsibly on their program.

'A strong scope not only reduces noise but also attracts quality researchers by helping them understand exactly what systems are in scope and what are not, meaning no time is wasted and no frustration is experienced in trying to understand what is allowed.' - How to attract security researchers to test on my bug bounty program?

For a deep dive into best practices, read 'Intigriti's Program Details'.

What are the benefits of Terms of Service (ToS) to a business?

Terms of Service provide a legal contract that combines rights, obligations, and liability. It is a legal agreement between both the Bug Bounty Platform and the researcher, as well as the company and the researcher, which can be made via the platform.

The goal is to define legal rights, as well as liability, and to establish clear rules to answer, 'What happens if something were to go wrong?', to protect all parties from legal exposure. This means that all elements from payment terms, property rights, dispute resolution, legal compliance, and account rights should be included.

Intigriti provides and describes the obligations between researchers and the Intigriti platform, and this is not something that customers can alter or edit.

Building a safer business with CoC, RoE, and ToS in place

> **"The Code of Conduct (CoC) establishes the expected standards of behavior for participants on the platform. The Terms of Service (ToS) define acceptable usage of the platform and prohibit actions that would compromise its integrity or operations. Building upon the ToS and CoC, the Rules of Engagement (RoE) specifically govern the scope and boundaries of security testing activities and apply those overarching platform rules to the individual customer environment, and define what is permitted within that context."**
>
> **Chris Holt, Strategic Engagement and Community Architect, Intigriti**

By putting all three elements into practice, through a Bug Bounty Program, VDP, or PTaaS, businesses can benefit from a structured, proactive, authorized, and legally protected form of security testing.

View the Intigriti Community Code of Conduct for specifics on collaboration and behavioural guidelines. And if you would like to take a deep dive, view the Researcher Terms and Conditions for more information on licensing, prohibited actions, obligations to reporting, confidentiality, data processing, and more.

If you have any questions regarding the content above or would like to talk with someone, contact the team today.

AUTHOR

Eleanor Barlow

Eleanor Barlow is a London-based Senior Cyber Security Technical Writer at Intigriti, with 9+ years' experience reporting on and writing for the cyber and tech sector. She specializes in data-driven content on cybersecurity and bug bounty intelligence, helping organizations benefit from the latest trends and insights.