Code of Ethics

1. Honor and respect the confidentiality of the information handled during a penetration test maintaining all sensitive information within the work environment.
2. Do not collect, store, give, sell, or transfer any kind of sensitive information gathered during penetration testing, including personal information such as names, usernames, e-mails, passwords, phone numbers, social security numbers, or any other personal unique identifier without the respective consent.
3. Understand the sensitivity of the information involved during penetration testing.
4. Inform all parties involved when confidential client information has been compromised prior to the penetration testing.
5. Do not purposefully compromise any client system or information nor allow them to be compromised in the course of my professional services.
6. Inform all stakeholders when confidential client information has been compromised during the penetration testing process.
7. Respect the limits established in the contract or Statement of Work testing only the items strictly established in such statement.
8. Be honest and truthful about the risks and exposures the client faces during and after the penetration test.
9. Do not purposefully compromise directly or indirectly the credibility of any parties involved, both employers and clients.
10. Ensure the full disclosure of all the risks encountered during the penetration test to all the involved stakeholders.
11. Participate only in projects of which I have full knowledge and experience, being honest about any limitations based on my experience and education.
12. Respect the law of the land and do not incriminate me, my employer, or my client, as a result of my ethical hacking activities.
13. Commit to staying current and up to date with the latest tools, techniques, and best practices to provide the best possible service to the client.