Adpoting a secure coding standard is very important, and essential in developing secure systems, reducing risk and vulnerabilities. With secure coding standards we can emphasis on best practices and guidelines that we all should follow to minimize security risks. The standards provide rules and recommendations, such as input validation, proper error handling, and secure authentication mechanisms, which help prevent common vulnerabilities like injection attacks, cross-site scripting (XSS), or insecure direct object references. We must assess the potential risks and impacts of security vulnerabilities and weigh them against the costs of implementing mitigation measures. By performing this evaluation we can help our companies prioritize their security efforts and allocate resources effectively. We can think of Zero Truest as an implementation of Triple A principiles. Zero Trust assumes that no user or system, whether inside or outside the network, can be inherently trusted. It requires continuous authentication, authorization, and verification of every user, device, and network interaction. Last but not least, we must implement and recommend security policies, and ensure everyone is onboard with it since security is the responsibility of us all.