The adoption of a secure coding standard is important to be adopted at some point in the SDLC. Security is something that is very important and needs to be made plans for throughout the entire time that a program is being made. You should always consider security when you are making something. It will only help you in the end and will always be better than not having one. This is the only way to make sure that not only you are safe and protected but anyone who uses the software and trusts you is safe and secure. You should never leave security till the end because then all the coding that you had done previously would have been pointless. When you go back and fix everything then you will have spent the same amount of time if not more to complete the program. There will also be the issue of whether it should have one.

The idea of evaluation and assessment of risk and cost. These are good to consider. You should always have an idea in your head with security with what is a good idea to protect more versus others. You will never be able to cover every single hole and if looked through long enough there will be a hole that will be found in your code. There is also just the idea that these should be mitigated and prevented as much as possible. The idea that would then go along with this is does the risk outweigh the costs. If it does, then you should go for it and if not then you shouldn’t go for it. The benefit of this is only good when it affects the software more than it hurts the software.

The idea of zero trust is a very easy one and yet a complex one. It is the idea that nothing is safe, and you can’t trust anything. This allows for the idea of a complete security lockdown. This means that you must make sure that every area has a lockdown point where if something breaks in then it can’t get past a certain point. This is a good idea when you consider all the little ins and outs of the system. It allows you to code while also keeping everything safe and secure. When you must fight every device, you must think and code out all the devices. This allows us to protect our users and our clients from harm.

The implementation and recommendation of security policies for any project is a big part and needs to always be discussed. There is a lot that goes into them. These are your standards, and these are the ways that you keep yourself, your company, and your client safe. These are the guidelines which help you and everyone else to know how to code as expected by your company. When you choose the policy by which you guide this company then it becomes a part of your identity and existence. There are multiple ways for a security policy to go about this but the main goal is to have one and implement it.