Adopting a secure coding standard is important because it is important to take security seriously at all levels. The reason that adopting a secure coding standard helps achieve this is because it allows for security to be a consideration throughout the entire development process. This ties into another point of not leaving security to the end. When security is left to the end, serious problems can arise. For example, it is easier to miss vulnerabilities when going back through code to fix potential vulnerabilities than it is to miss vulnerabilities when a developer is coding with the idea of preventing vulnerabilities in the first place. Adopting a secure coding standard and not leaving security to the end are major parts of a DevSecOps pipeline.

Evaluating and assessing risks is important because it allows for the prevention of data breaches. Evaluating and assessing risks allows developers to examine potential vulnerabilities in their code. This makes code more secure, which has the benefit of mitigating future costs that could be incurred because of vulnerabilities. While there might be a resource cost upfront of mitigating security risks, spending the resources to do that now can prevent even higher costs later that come from dealing with a data breach.

A policy of zero trust is a good idea because cybersecurity vulnerabilities can come from anywhere. Even areas where it seems like no attacks can occur can be vulnerable to data breaches. It is important to verify that every area is as secure as possible. Assuming that nothing is secure until steps are taken to secure it allows for developers to take further steps to avoid data breaches.

All the security policies mentioned can be implemented in a DevSecOps framework, and they each have their own advantages compared to a system in which they are not implemented. Even though it may take time and resources to implement them, it is worth doing because the risk is that even more time and resources are spent fixing vulnerabilities and dealing with the fallout of something like a data breach.