Security in any project is one of the most important steps. One of the first things that needs to be done is adopting a secure coding standard. This helps to keep the code safe and compliant. During the planning phase, the team should go over the programming languages to be used and develop coding standards for those languages. If a program is not compliant with a coding standard, it is more likely to have vulnerabilities. Security should begin being included at the beginning of the development lifecycle. Programs that have security included at the beginning are far less likely to have issues later in the development lifecycle. The best thing to practice is keeping security first instead of leaving it to the end.

Mitigating any vulnerabilities that are found as soon as possible saves time and money. Any vulnerabilities that are found and not fixed as soon as possible are at risk of being much bigger problems if they are exploited. A system breach can cause distrust of the company, legal issues, and the loss of a lot of money. While incorporating security and mitigating vulnerabilities cost a company money, waiting until there is a breach will cost a company a lot more money and a lot more problems. It is important to run unit tests, fix compiler warnings, and use static analyzers during development.

Zero Trust is a security model where no user, device, workload, or system should be trusted, regardless of their location. This is very important to implement in today’s world of remote work. Allowing remote work is very beneficial to employees and companies, however with people working all over the country and on multiple servers and networks there is a much greater security risk. This is where a Zero Trust model is great. This model verifies, barricades, and isolates everything in the system. Thus, if an attacker gets into a system, the breach will be more isolated and valuable assets won’t get taken (Check Point Software Technologies, Ltd, 2019).

One of the best policies when implementing security is do not wait. Training employees on security policies and ensuring those policies are followed is one of the biggest steps. Employees should be trained on the most common types of attacks and how to prevent them. Developing and implementing Triple-A, Encryption, and Defense-In-Depth are all great ways to ensure a system stays secure.

References:

Check Point Software Technologies, Ltd. (2019). *What is Zero Trust Security?* [Video]. YouTube. Retrieved from [What is Zero Trust Security? - YouTube](https://www.youtube.com/watch?v=1D5mg9an19o)

Seacord, R. “Chapter 9. Recommended Practices.” Secure Coding in C and C++, 2nd ed., Software Engineering Institute of Carnegie Mellon, 2013.