While writing code security should be at the forefront of every programmer’s mind. The only people who should have access to the given system are those that are authorized to use it. Having secure coding standards are a sure-fire way to keep what is important in the primary view of those creating the programs or systems. Default and Deny should be the first course of action when it comes to access on a chosen system. That should be written as the first line of defense to keep intruders out. Also, when creating programs and outside code is used, that code should always be validated as using outside code could potentially leave an unintended backdoor into an otherwise secure system.

When writing code, using the compliers most stringent checks and highest warning level is the safest best. While it may be annoying at times, the compiler is doing its job and showing the programmer where the holes are. Layering of defenses, with each line standing on its own but also working in tandem with other lines of defense is another best practice that should always be implemented through the life cycle of any given program.

Risk assessment is one of those things that varies from programmer to programmer but there should always be a standard that each person in the organization follows so that every risk is assessed the same way and to the same standards so that very little if at all falls through the cracks and gets the required amount of bandwidth it should. Mitigation to reduce the impact of any disaster should also be high on the list of any programmer. No system is full proof, there will always be a way in, there should be a plan to lessen the impact and stem the tide for when the disaster does occur. An ounce of prevention is worth a pound of the cure.

Trust but verify is another way of saying zero trust. Everyone that uses that system should be kept out at all cost until they have authenticated themselves and thereby been authorized to use the system. It is significantly easier to grant access to those who are trusted than try to work at getting the unwanted out when everyone has access.

There are a few items to recommend when it comes to security polices: Always identify the risks. It is good to know who and why someone will want your data. Compartmentalize data, not all data requires the same amount of security. Limit the most sensitive data to the most demanding of security protocols. When creating a security policy, involve as many of the staff as possible, as each person can give a different idea as to how threats may occur or what needs to be protected. Following suit, set clear boundaries and should those boundary lines be crossed, set clear penalties and stick to them.