CS 405 Project Two Script Template

Complete this template by replacing the bracketed text with the relevant information.

Slide Number	Narrative
1	My name is Brandon Womack, This is my security policy presentation for Green Pace.
2	This model is to give an overview of the detailed methods of defense that we use in our work to maintain a solid blueprint to secure coding. WE strive to maintain the highest quality services in secure coding.
3	Secure Coding standards come with certain levels of vulnerability to measure the impact of that certain standard. There are threats that are very likely to occur in most situation then there are those that should be given proper attention but aren't as likely as others. Both likely and unlikely instances come with low and high priorities levels as well.
4	There are 10 base principles to secure coding. Always remember to validate input data, heed all compiler warnings you may receive through development and debugging. Build and design for security when in development. Always keep things simple yet effective. Deny access to systems by default as a standard. Adhere to principles of least privilege. Sanitize data sent to other systems to keep connections and transfers between other systems safe. Always practice defense in depth because you can never be TOO secure. And remember to always use effective quality assurance techniques and be sure to adopt a secure coding standard that is efficient and effective.
5	We comply with a few important coding standards here a Green Pace our top ten standards are: 1. Do not cast to an out-of-range enumeration value 2. Use valid references, pointers, and iterators to reference elements of a container 3. Do not attempt to create a std::string from a null pointer 4. Do not store already-owned pointer value in an unrelated smart pointer 5. Properly deallocate dynamically allocated resources 6. Use a static assertion to test the value of a constant expression 7. Handle all exceptions thrown before main() begins executing 8. Do not alternately input and output from a file stream without an intervening positioning call 9. Do not invoke virtual functions from constructors or destructors 10. Value returning functions must return a value from all exit paths

Slide Number	Narrative
6	Our encryption policies are alsoa prioritized standard here at green pace. With encryption in rest, that is designed to keep attackers from accessing unencrypted data because the data would be encrypted on disk. Encryption in flight is the process of encrypting data while the data is in transit within the system. Encryption in use is the comprising of data at rest and in motion.
7	We also keep a high standard with our Triple-A policies. The first A is for authentication, this is the process of identifying and verifying the users identity. The second A is for authorization for when the user is confirmed. This determines the level of access the individual user has once they have been confirmed and the system has been accessed. This can include whether or not the user can read, create, delete or modify files, users and databases within the system. The final A is for Accounting. This just keeps track of all that the individual user does within the system so that they can be held accountable for all actions when they have access.
8	Our unit test practices come early and often through out the development process to ensure that we have secure functioning code. Ex. Limiting the number of characters within a user input string to prevent buffer overflow.
9	The DevSecOps pipeline is a secure coding method that has a full circle approach to enforcing a policy that has an infrastructure built on efficiently keeping code secure.
10	This is a solid structure for the system, I would just always be mindful of defense in depth and making sure that you are testing early and often to detect any flaws or vulnerabilities so that we can be able to catch those bugs and errors early.
11	There will always be risk when coding because nothing can be 100% secure. Always assume that there are threats and flaws in the system and stay persistent with keeping up with all of today's common threats and prevention techniques, so continuing education is highly critical to the success of this policy. The benefits to this policy would be that we strive to do what we can to stay current and up to date to guarantee the highest quality security for our clients.
12	Keeping up with all the security threats and trends is a critical piece to maintaining the level of security we promise. We keep everything simple yet effective to get the job done. Things such as SQL injection practices to prevent attackers from manipulating the databases within your system is just one of the many standard we adhere to provide quality service.

Slide Number	Narrative
13	In conclusion, With the principles and standards mentioned within this presentation we can conclude that most of all the important topics were covered to display our plan to create and maintain a secure and proficient programing. We also have adopted a zero-trust policy when it comes to accessing things inside and outside of the company network to maintain security and privacy to keep all sensitive information safe and secure for all parties involved.