# CS 405 Project Two Security Policy Presentation

**https://youtu.be/UGAcYm-mj5U**

| **Slide Number** | **Narrative** |
| --- | --- |
| **1** | Hello, I am Gregory Greene, a Computer Science Major at Southern New Hampshire University. This presentation will cover Security Policies for Green Pace. |
| **2** | Defense in Depth is an approach to security in which developers implement multiple layers of defense in order to prevent different possible vulnerabilities in a system. |
| **3** | Here we see our Threats Matrix and our Coding Standards sorted by Likelihood and priority level. |
| **4** | Our 10 Principles include:   * Validate Input Data * Heed Compiler Warnings * Architect and Design for Security Policies * Keep it Simple * Default Deny * Adhere to the Principle of Least Privilege * Sanitize Data Sent to Other Systems * Practice Defense in Depth * Use Effective Quality Assurance Techniques * Adopt a Secure Coding Standard |
| **5** | Here we can see our coding standards sorted. When reviewing standards, we must prioritize based on Severity and Likelihood. Remediation Cost should be considered but should not be prevent a standard from being implemented. |
| **6** | Our 3 encryption policies include:  Encryption in Use which protects data created, edited, or otherwise defined as in-use.  Encryption in Rest which protects stored data, typically through hard drives, smartphones, computers, and cloud systems.  Encryption at Flight which protects data that is being transmitted either inside or outside a network. |
| **7** | The Triple-A Policies are Authentication, Authorization, and Accounting.  Authentication ensures a user is who they say they are through identity verification.  Authorization defines the access rights and privileges of each user, typically through role assignments.  Accounting processes and tracks user activity within a system. This tends to include timestamps, accessed resources, and data transfer information. |
| **8** | Unit testing is done to verify components of a program to ensure it functions properly when called upon by a user. Some unit testing methods include; Black Box testing, White Box testing, Agile testing, Grey Box Testing, and Ad-hoc Testing. |
| **9** | Here we can follow the process behind Automation.  The path here is as follows:  Assess and plan, Design, Build, Verify and Test, Transition and Health Check, Monitor and Detect, Respond, and Maintain and Stabilize. |
| **10** | DevSecOps is considering application and database security from the start of development. This mindset puts security first and causes developers to consider different types of security throughout the development process.  Some tools used include Parasoft, CPPCheck, and Clang. |
| **11** | Benefits of Early Action and Correction include:  Preventing threats to the system, Creating a secure infrastructure, reducing the amount of testing necessary, and mitigating possible damage and cost.  Risk of Delayed Action includes:  Financial Cost, Loss or spread of customer information, and potential damage to company reputation. |
| **12** | Some recommendations for development include:   * + - Security Policies need to be frequently audited and updated.     - Early implementation of security policies will reduce cost and time spent debugging.     - Implement Defense in Depth to include layers of security against various forms of attack.     - If security is a major concern, an outside contractor can be hired to review and test security policies implemented. |
| **13** | In conclusion, implementing security policies early through a DevSecOps mindset can help prevent unauthorized access. Defense in Depth and a “No One is Safe” mindset can help to layer security and increase types of threats being prevented. When considering possible security policies “Motive is Mystery” should be remembered to be open-minded to possible security measures. |
| **14** | References used for this presentation include the following:  IBM Documentation – Processing AAA Policies  What is DevSecOps?  And  What is Encryption and How Does it Work? |