# CS 405 Project Two Script Template

Samuel Bailey

August 9, 2021

Project Two Script

https://www.youtube.com/watch?v=nwHILoz8QT4

| **Slide Number** | **Narrative** |
| --- | --- |
| **1** | Hello my name is Samuel Bailey, I work for Green Pace and today I will be talking to you about our new security policies. |
| **2** | Our new security policy is using the Defense in Depth methodology. Which basically means there is levels of defense for our organization information security implemented by our organization. |
| **3** | This is a small example of a threats matrix or security matrix. This shows different risks that we have identified and compartmentalized. What I mean by that is something that is likely to happen is phishing but something unlikely to happen is our entire repo disappearing. |
| **4** | As an organization we want to setup principals of things that we want to be aware of and use. Some of those are <List principals> and this list was created from Carnegie University. |
| **5** | With those principles we also want to setup long lasting coding standards for all of our dev’s to use. Some of those include <List standards> |
| **6** | Moving on we have our encryption policies for Rest In Flight and In Use. <List how they work> |
| **7** | Next we have our Triple A policies, which are Authentication, Authorization, and Accounting. <Describe how they work> |
| **8** | As dev’s we always want to test our code in almost every way possible. Here we have some examples of unit testing, each language has a different way to do it and different ways to test all together. But here is an example of 4 unit test where 3 pass and one fail. |
| **9** | Just creating code isn’t enough for making sure it works and using it in production. For that assurance that it works how it’s suppose to we use an Automation process/summary. This is our process to build test, design and things of that sort. |
| **10** | For tools that we use it will be different for every project. But some base line tools we are going to use is a REPO. And a code quality tool we can use to check is SonarQube. As well as our Continuous Integration / Continuous Deployment |
| **11** | There isn’t many risks that come with DID. These risks come more from the users and how fast they can act on the principals that are in place. For example if a hacker takes control of our site we need to act immediately and take control back. The longer we wait the less our policy is going to do for us. |
| **12** | The best recommendation that I have for this policy is to give the users timed access. Force them to renew their authentication every single day and every single time they login to their computer. Although this does come with some cons of user satisfaction. |
| **13** | In conclusion the DID process is one we should adopt. At this current time I don’t see any downfall of using this process. Although things always change and there will come a day where we need to adopt a new process but not as of now. |
| **14** | My only reference is from the Carnagie University website from our resources page. |