# CS 405 Project Two Script Template

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

| **Slide Number** | **Narrative** |
| --- | --- |
| **1** | Hello my name is ian, and here I am going to present too you my security policy presentation for green pace |
| **2** | Defense in depth is where you use security mechanisms carefully and thoughtfully layered in a manner that will create stronger protection against security risks ad vulnerabilities in a system. This security in layers prevents other layers from getting breached when one has been breached |
| **3** | Here is the threats matrix I created for this presentation where there is two likely security breaches with high harm potential which are STD-003-CPP and STD-005-CPP, this would put these as high priorities. STD-007-CPP is a probable threat with low harm, while STD-002-CPP, STD-004-CPP, STD-009-CPP, and STD-010-CPP are probable threats with high harm potential putting them at a higher priority than STD-007-CPP. Unlikely threat with low harm is STD-006-CLG, then an unlikely threat with moderate harm potential is STD-008-CPP, while STD-001-CPP is unlikely but has a high harm potential making it more crucial too fix than the previous two mentioned in the unlikely threats. |
| **4** | Here are the 10 principles with their threat that corresponds to them |
| **5** | This page includes a diagram that shows each threat, its severity, likelihood, remediation cost, priority, and level which all makes it easy to intake each threat and their corresponding information |
| **6** | Encryption in rest is where you protect stored data.  Hard drives, phones, computers, cloud, etc.  Encryption in flight is where you protect data that is moving or being transferred.  devices within a network or moving outside a network.  Encryption in use is where you protect data that is being created, edited, or considered “in-use”  protects data prior to being used or created |
| **7** | Authentication- confirming one’s identity  ensure that a person is who they really claim to be.  Authorization- Specifies the rights and privileges of users  controls what a user can and cannot access  Accounting- this is the process of keeping track of activity within a system including timestamps and resources accessed.  all activity is tracked and documented |
| **8** | Unit testing- verifies and validates components of a program or application to make sure that the app will work as intended. |
| **9** | Here is a image that summarizes the automation process of dev secops. This includes two phases, the pre-production phase and the production phase which each has its corresponding parts that make up the devsecops pipeline |
| **10** | Devsecops is where you think about application and infrastructure security from the beginning all the way to the end of development. |
| **11** | * Risks- * Risks data * Risks customer trust * Risks financial cost * Risks potential future damage * Benefits- * Mitigates damage * Prevents further threat * Creates strong and consistent security |
| **12** | Reccomendations I would make is more frequent testing from outside sources to ensure security is up to real-world standards as well as get an outside perspective on their security. |
| **13** | There are a couple things I can come to conclusion of after this, Adopting best practices and coding standards, practicing defense in depths as well as the triple a’s will allow for better security as well as protect against future attacks and if said attack were too happen, the damage would be mitigated as much as possible. |
| **14** | And finally here are my resources I used when creating this. |