Project Two Script

# Title Slide

Hello! I am Li Pintar and today I will be giving a presentation on security policies at Green Pace.

# Overview Slide

Green Pace’s security policy outlines a set of standards derived from the 10 security principles. We can practice defense in depth with layers of security which will follow the uniformly defined, implemented, governed and maintained standards.

# Threats Matrix Slide

The threats matrix is a tool that helps with visualizing the probability in comparison to the potential impact of security risks. There are two variables we consider when assessing security risks: likelihood of occurring and priority of the risk. Mitigating risk takes time and resources which can limit the amount of risks that can be addressed. Using the threats matrix to assess risks allows us to create a mitigation strategy that prioritizes the biggest risks.

# 10 Principles Slide

These are the 10 security principles. Below each of them are the standards that relate to them.

# Coding Standards

Here we have the coding standards in order of priority. The standards were prioritized by assigning a weight to the likelihood, impact, and cost, adding up the weight of all three factors, and organizing the standards accordingly.

# Encryption Policies

Encryption at rest is when data is secured using encryption to prevent unauthorized access to sensitive data while it is stored or "at rest".

Encryption in flight is when data is secured using encryption to prevent data theft of sensitive data while it is in transit through a flightnetwork or "in flight"​.

​Encryption in use is when data is secured through encryption to prevent unauthorized access to sensitive data while it is at rest and in transit.

# Triple-A Policies

Authentication allows businesses to control who can access their system .

Authorization comes after authentication. This is when user authentication is verified.

Accounting is checks and balances to monitor the system and track usage and collection of data.

# Unit Testing

Unit tests can act as one of the layers of security.

This unit test verifies that five values can be added to the collection.

This unit test verifies that the capacity can be increased without affecting the size of the collection.

This unit test verifies that an exception is thrown when the index is out of range.

And this last unit test verifies that an exception is thrown when the index is below zero.

# Automation Summary

Green Pace aims to integrate security throughout the entirety of the software development lifecycle. In every phase, security will be considered.

# Tools

Many different tools are utilized when implementing security measures. This slide lists a few.

# Risks and Benefits

Waiting to implement defense in depth can potentially be more costly than investing the time and resources initially. Time and resources will be spent chasing security breaches that could have been prevented with the same resources and on top of that, vulnerable data could already be compromised. By creating layers of security from the beginning, time and resources can be spent on maintaining the product rather than patching holes late. While this approach could potentially lead to resources being spent on mitigating vulnerabilities that might not be exploited, if the risk vs impact estimation is accurate, the benefits will outweigh the risks.

# Recommendations

My recommendations are:

.Implement security measures to software updates as well​

.Have a plan for addressing a breach in security​

.Educate team members on security coding standards​

.Gather requirements with security so that the security needs are fully understood​

.Adhere to coding standards consistently

# Conclusions

In conclusion, it is best to implement defense in depth throughout the entirety of development and a strategy should be formed for how we deal with security breaches after they occur.