**Project Proposal:**

**“PolicyCraft”**

**1. Project Title, Group Numbers and ID**

**Project Title:** PolicyCraft (a Personalized Security Policy Generator)

**Member 1:** Anas Khan (21k4761)

**Member 2:** Shah Muhammad (21k3557)

**2. Proposed Project Description:**

Cyber security threats are a growing concern for individuals and businesses of all sizes. However, creating effective security policies can be complex and time-consuming, often requiring specialized knowledge. This project proposes the development of a user-friendly tool, the Personalized Security Policy Generator, to address this challenge.

The Personalized Security Policy Generator will be a program designed to empower users to create customized security policies.

It will achieve this through the following functionalities:

**Network Assessment:** Users will be guided through a process of providing information about their network setup, including the size and type of network (home, office), connected devices (laptops, desktops, IoT devices), and internet usage patterns (work, entertainment, online transactions).

**Risk Assessment:** Based on the user's network assessment data, the application will analyze potential security risks. This analysis will consider factors like data sensitivity (financial data, personal records), outdated software or weak passwords on connected devices, and potential external threats based on the user's industry or online activity.

**Personalized Recommendations:** Leveraging the risk assessment, the application will suggest appropriate security controls tailored to the user's specific needs. These recommendations may include basic measures like strong passwords, enabled firewalls, and up-to-date antivirus software for home networks, or more granular controls like user access controls and data encryption for small businesses.

**Security Policy Generation:** The application will translate user choices and recommendations into a clear and concise security policy document. This document will outline the chosen security measures and provide explanations for their implementation.

**3. Plan of Work (Next 5 Weeks)**

**Week 1 (20%)**

**Collaboration (100%)**

* Finalize the design of the overall user interface (UI) with wireframes or mockups for key functionalities (network assessment, risk assessment display, security control recommendations, and security policy generation).
* Define a list of pre-defined security controls for different user profiles (home network, small business).

**Individual Work (40%)**

Shah Muhammad: Start developing logic for analyzing user-provided network information for the risk assessment module (20%).

Anas Khan: Choose a Python UI library (e.g Tkinter or PyQt) and begin developing core UI elements using the library (20%).

**Week 2 & 3 (40%)**

**Collaboration (30%)**

* Refine the UI design based on initial discussions and potential challenges.
* Integrate the risk score with the pre-defined security control library.

**Individual Work (70%)**

Shah Muhammad: Finalize the logic for analyzing user-provided network information and assigning risk scores based on predefined criteria (data sensitivity, device vulnerabilities, external threats) (50%).

Anas Khan: Continue developing core UI elements and implement functionalities for user interaction and data input within the UI for network assessment and risk assessment display (50%).

**Week 4 & 5 (40%)**

**Collaboration (40%)**

* Develop logic to suggest appropriate security controls based on the user's risk profile.
* Design a security policy template with placeholders for user choices and recommendations.

**Individual Work (60%)**

Anas Khan: Develop logic to populate the security policy template with user-specific information for security policy generation (50%).

Shah Muhammad: Implement functionalities for security control recommendations and integrate them into the UI (50%).

**4. References**

**National Institute of Standards and Technology (NIST) Special Publication 800-53:**

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>

**Center for Internet Security (CIS) Controls:**

https://www.cisecurity.org

**Python UI Libraries:**

**Tkinter Documentation:**

https://docs.python.org/3/library/tkinter.html

**PyQt Documentation:**

<https://riverbankcomputing.com/software/pyqt/intro>