**Information Security Policy Plan**

TB Patient’s Appointment System

**Prepared by:**

Keyan Andy Delgado

Jener Kevin Ogatis

Lynch Nico Futolan

**Introduction**

**SECURITY MEASURE FOR LOGIN**

* **Password Validator**: This feature ensures that the password entered by the user meets certain criteria for strength, such as length, complexity (use of numbers, symbols, upper and lower case letters), and uniqueness. This helps to protect user accounts from being easily compromised.
* **Limited Login Attempts**: This feature restricts the number of times a user can attempt to log in within a certain time period. If the maximum number of attempts is exceeded, the user account may be temporarily locked. This helps to prevent brute force attacks.

**ROLE-BASED ACCESS CONTROL (RBAC)**

* **Admin Approval**: This feature requires an administrator to approve certain actions or access requests made by users. This adds an extra layer of security by ensuring that only authorized actions are performed.
* **Logs**: These are records of events or actions that have occurred within the system. They can be used to track user activity, monitor system health, and investigate security incidents.

**NETWORK SECURITY POLICY**

* **Auto-Logout**: This feature automatically logs out a user after a certain period of inactivity. This helps to prevent unauthorized access if a user leaves their device unattended.
* **Block Session Bypass**: This feature prevents users from bypassing the login process and accessing the system without proper authentication.
* **Recaptcha**: This is a security service that protects the system from spam and abuse by distinguishing human users from bots. In the context of the TB Appointment System, it is used during login and when creating appointments.
* **SSL Certificates:** These encrypt the data transferred between the user’s browser and the server, preventing it from being intercepted and read by third parties1.

**DATA ENCRYPTION**

* **AES-256 Encryption**: This is a method of data encryption that uses a 256-bit key to encrypt and decrypt data. It is one of the most secure encryption methods and is widely used in many types of security protocols. In the context of the TB Appointment System, it is used for encrypting the account number. This ensures that even if the data is intercepted, it cannot be read without the encryption key.