# LIST OF SECURITY FEATURES

## Authentication System

The authentication mechanism validates user credentials during login, ensuring only verified customers or the administrators/managers gain access to the system. Users must provide correct login credentials, and successful authentication results in a persistent but time-limited cookie. This discourages automated guessing attacks and helps protect user accounts from unauthorized access. Each customer is responsible for his own subscriptions and payments. So, authentication is made necessary, after which, only the subscriptions and payments for the respective customers are shown to them.

## Role Based Access Control

Access to system functionalities is strictly regulated through role-based permissions. Different user roles (Administrator, Customer, Customer Payment Manager, etc.) have dedicated dashboards with role-specific features. The system verifies user roles before granting access to any restricted page, preventing unauthorized users from accessing sensitive operations. This multi-tiered access structure is enforced through role cookies effectively minimizing the risk of privilege escalation.

## Parameterized Queries

The application exclusively uses parameterized SQL queries for all database operations. This security measure effectively neutralizes SQL injection threats by separating SQL commands from user-supplied data. Every database interaction, whether reading or modifying records, employs this protection to maintain data security while preserving application functionality. This implementation spans all data access layers of the application.

## Input Validation

The application enforces strict input validation to ensure only properly formatted data is processed. This includes password complexity requirements (minimum length, uppercase, lowercase, and numeric characters) to prevent weak credentials. Required field validation ensures no empty submissions are accepted, maintaining data consistency. Additionally, auto-generated customer IDs prevent manual ID manipulation, reducing risks of privilege escalation or impersonation attacks. These validations are implemented using ASP.NET validation controls.

## Cookie Management

User sessions are managed through carefully configured cookies with strict security attributes. These session tokens include expiration policies that automatically terminate sessions after 24 hours, reducing the window of opportunity for session hijacking attacks.

## Restricted Login Attempts

To prevent brute-force login attempts, the application limits the number of consecutive failed login attempts to three. If a user fails to log in after three tries, the login form (including the username and password fields) is disabled for a duration of two minutes. This mechanism is implemented using cookies that track both the number of failed attempts and the lockout period.

## HTTPS Encryption

All communication between clients and the server is encrypted using HTTPS protocol. This encryption safeguards sensitive data like login credentials and payment information from interception during transmission. By establishing secure channels for all data exchange, the system effectively prevents man-in-the-middle attacks and ensures data integrity throughout user interactions. HTTPS is enforced via the hosting environment somee.com.