**XÁC ĐỊNH CÁC BIỆN PHÁP BẢO MẬT NHƯ XÁC THỰC, KIỂM SOÁT TRUY CẬP**

1. **Xác Thực Người Dùng**:

a. Xác Thực Một Lần (Single Sign-On - SSO):

Cho phép người dùng đăng nhập vào nhiều ứng dụng với một tài khoản và một mật khẩu duy nhất.

b. Xác Thực Hai Yếu Tố (Two-Factor Authentication - 2FA):

Yêu cầu người dùng cung cấp hai phương tiện xác thực khác nhau để đảm bảo tính bảo mật cao hơn.

c. Xác Thực Biometic:

Sử dụng các phương tiện như quét vân tay hoặc nhận dạng khuôn mặt để xác thực người dùng.

2. **Kiểm Soát Truy Cập**:

a. Quản Lý Phiên (Session Management):

Kiểm soát thời gian tồn tại của phiên đăng nhập và hủy phiên sau một khoảng thời gian không hoạt động.

b. Kiểm Soát Quyền Truy Cập (Access Control):

* Phân quyền cho người dùng dựa trên vai trò hoặc nhóm người dùng.
* Áp dụng kiểm soát truy cập tới các tài nguyên như danh sách phòng trọ hoặc chức năng như chỉnh sửa thông tin cá nhân.

c. Điều Kiện Truy Cập (Conditional Access):

Xác định các điều kiện để kiểm tra và quyết định quyền truy cập của người dùng, như địa chỉ IP, thiết bị hoặc vị trí địa lý.

d. Ghi Nhật Ký Truy Cập (Access Logging):

Ghi lại mọi hoạt động truy cập vào hệ thống để theo dõi và phát hiện các hành vi không bình thường hoặc tấn công.

e. Tính Toàn Vẹn Dữ Liệu (Data Integrity):

Bảo vệ tính toàn vẹn của dữ liệu bằng cách đảm bảo rằng dữ liệu không bị sửa đổi hoặc biến đổi trái phép.

f. Bảo Mật Cơ Sở Dữ Liệu:

Sử dụng các cơ chế bảo mật như mã hóa dữ liệu, kiểm tra ràng buộc SQL, và quản lý người dùng và vai trò một cách cẩn thận.

g. Kiểm Tra Định Kỳ (Regular Audits):

Thực hiện các kiểm tra định kỳ để đảm bảo rằng các cơ chế bảo mật đang hoạt động đúng như kỳ vọng và không có lỗ hổng nào được bỏ qua.