**NHẬP MÔN CNPM CHƯƠNG 2:**

1. **Xác định các yêu cầu phi chắc năng:**
   1. ***Giao diện người dùng***

* Thiết kế giao diện đơn giản và trực quan: Người dùng muốn giao diện đơn giản, trực quan và dễ sử dụng để có thể theo dõi, tìm kiếm một cách dễ dàng. Thiết kế nên được tổ chức thành các danh mục để dễ dàng điều hướng giúp người dùng có thể tìm thấy thông tin mình cần một cách nhanh chóng.
* Tương thích với nhiều thiết bị và màn hình khác nhau: Tương thích với các thiết bị đa dạng giúp khách hàng truy cập vào website từ bất kỳ thiết bị nào mà họ sử dụng. Thiết kế nên tương thích với nhiều loại màn hình khác nhau để đảm bảo rằng giao diện sẽ hiển thị ổn định và chuyển đổi trơn tru trên tất cả các thiết bị và màn hình.
* Tốc độ tải trang nhanh: Người dùng mong muốn giao diện được tối ưu hoá để giảm thiểu thời gian tải trang. Tốc độ tải trang nhanh giúp gia tăng trải nghiệm của người dùng và ngăn chặn họ từ việc rời bỏ website do việc tải trang quá chậm.
* Thân thiện với thiết bị di động: Thân thiện với thiết bị di động là một trong những yêu cầu phi chức năng quan trọng. Không chỉ dễ sử dụng trên máy tính, giao diện cũng phải thân thiện và dễ sử dụng trên các thiết bị di động nhằm làm tăng khả năng truy cập, tiện lợi cho người dùng.
* Sử dụng hình ảnh và video ấn tượng: Hình ảnh và video là một phần quan trọng của giao diện người dùng.
  1. ***Tính bảo mật và các ràng buộc***

Khi hệ thống lưu trữ, truy xuất dữ liệu cá nhân như thông tin khách hàng, thông tin thẻ, các thông tin riêng tư, chúng ta cần phải có biện pháp đảm bảo an toàn những dữ liệu này.

* Xác định vai trò:
* Toàn bộ ứng dụng không chỉ có một mức độ bảo mật.
* Người dùng cuối chỉ cần quyền truy xuất giới hạn vào hệ thống, người thao tác viên cập nhật và người dùng có quyền truy cập cao hơn ở mọi cấp độ.
* Bảo mật dựa trên vai trò là kĩ thuật dùng để cấp quyền mức độ bảo mật khác nhau tương ứng quyền hạn và độ chuyên nghiệp của mỗi người dùng trong hệ thống.

**Lưu ý:** Nhận biết những lớp chính của những người dùng cần truy cập đến ứng dụng của chúng ta. Gán tên vai trò cho mỗi lớp người dùng. Cuối cùng, gán mức độ tối thiểu có thể truy xuất đến mỗi vai trò. Mỗi lớp người dùng nên có đủ quyền truy xuất đến công việc của họ và không nhiều hơn.

* Xác định môi trường bảo mật hệ thống
* Độ bảo mật không bị giới hạn người dùng hệ thống.
* Chỉ người dùng đăng nhập vào ứng dụng, ứng dụng phải “login” để kiểm soát tài nguyên chia sẻ như tập tin, dịch vụ hệ thống, cơ sở dữ liệu.
* Mức độ kiểm soát của ứng dụng được gọi là ngữ cảnh bảo mật.
* Chúng ta cần phải làm việc với nhiều người dùng khác như quản trị mạng, cấp quyền truy xuất phù hợp ứng dụng để chia sẻ tài nguyên.
* Xác định ảnh hưởng bảo mật

Nếu công ty có sẵn cơ chế bảo mật thay vào đó hệ thống của chúng ta nên điều chỉnh cho phù hợp với cơ chế đã có. Nếu chúng ta đang thực thi hệ thống bảo mật mới hay một hệ thống khác, cần phải phân tích tác động của hệ thống trên hệ thống hiện tại:

* Hệ thống mới có làm hỏng chức năng của phần mềm hiện tại?
* Hệ thống đòi hỏi phải hỗ trợ thêm một phần người dùng - đăng nhập mở rộng?
* Hệ thống sẽ khóa một vài người dùng trên những tập tin hay những tài nguyên mà họ được truy cập trước đây.
* Kế hoạch vận hành
* Khi tổ chức phát triển và thay đổi, người dùng mới được thêm vào, người củ được cập nhật và bỏ đi.
* Những thao tác này đòi hỏi thay đổi CSDL bảo mật, đó là nơi thông tin người dùng và quyền hạn truy cập của họ được lưu.
* Những thông tin này được lưu trữ hiện thời.
* Kế hoạch kiểm soát và ứng dụng
* Một hệ thống bảo mật tốt không là cơ chế thụ động. Thay vào đó, chứa chức năng trợ giúp kiểm soát hoạt động của hệ thống cho vấn đề bảo mật.
* Vấn đề chung của chức năng này là nhật kí.
* Toàn bộ thao tác của hệ thống có thể được ghi nhận hầu như toàn bộ sự kiện liên quan đến bảo mật hệ thống.
* Có thể ghi nhận mỗi khi đăng nhập, truy xuất đến mọi tài nguyên nhưng điều này hiếm khi hiệu quả. Thường chúng ta sẽ ghi nhận một số tập thông tin này như việc cố gắng đăng nhập lỗi.
* Xác định mức độ yêu cầu bảo mật
* Bảo mật cũng giống như những phần khác trong thiết kế ứng dụng, là sự cân nhắc giữa hiệu quả và chi phí.
* Nếu hệ thống không lưu những dữ liệu có tính nhạy cảm cao.
* Cách tốt nhất để triển khai hệ thống đó là “giữ sự xác thực của người dùng” đòi hỏi lưu trữ.
* Nếu chúng ta lưu trữ thông tin cần cho bảo mật, chi phí cho bảo mật thông tin đặc biệt phải được kiểm chứng.
* Không có hệ thống nào bảo mật 100%. Chúng ta phải xác định mức độ rủi ro bảo mật có thể chấp nhận được.
* Độ rủi ro bảo mật diễn tả tỉ lệ phần trăm tương xứng khả năng mà bảo mật hệ thống không bao giờ đạt đến.
* Điều đó có thể nhưng chi phí phí tốn để xây dựng hệ thống bảo mật 99%.
* Chúng ta hay khách hàng phải xác định mức độ rủi ro có thể chấp nhận được dựa trên dữ liệu nhạy cảm của hệ thống.