PHỤ LỤC

YÊU CẦU CỦA PHẦN MỀM TRỢ LÝ ẢO HỖ TRỢ THẨM TRA THẨM ĐỊNH

(Kèm theo Công văn số 4376-CV/VPTU ngày 04/12/2024 của Văn phòng Thành ủy)

I. Yêu cầu chung:

Hệ thống thông tin phải tuân thủ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ, Thông tư số 12/2022/TT- BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông về quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 nhằm đảm bảo an toàn thông tin trên môi trường máy tính, mạng máy tính và Quyết định số 742/QĐ-BTTTT ngày 22/4/2022 của Bộ TTTT ban hành yêu cầu an toàn cơ bản đối với phần mềm nội bộ.

** Giải pháp kỹ thuật phải đáp ứng các yêu cầu sau:*

- Tính khả thi: Giải pháp đưa ra phải giải quyết được các yêu cầu đang đặt ra, phù hợp với điều kiện thực tế. Giải pháp nâng cấp phải đảm bảo tính khả thi của dự án sao cho hệ thống khi nâng cấp cần phải dễ dàng trong việc triển khai cũng như khi vận hành tại thời điểm sau.

- Hệ thống cho phép người sử dụng (bao gồm cả các đồng chí là Lãnh đạo Thành ủy, thành viên các cuộc họp) được phân quyền khai thác, sử dụng theo từng hồ sơ trình.

- Tính hiện đại: Các giải pháp đưa ra dựa trên các công nghệ mới hiện đại và đang được sử dụng phổ biến.

- Tính chuyên môn: Các giải pháp do các chuyên gia có kinh nghiệm xây dựng. Các chuyên gia và kỹ sư hệ thống phải có đầy đủ kiến thức cũng như kinh nghiệm để giảm thiểu những rủi ro và khó khăn khi triển khai.

- Tính tương thích cao: phải tương thích với các mô hình khác đang được sử dụng rộng rãi.

- Tính bảo mật: Ngoài các thông tin được đăng tải rộng rãi thì các giải pháp phần mềm phải đảm bảo tính an toàn và nguyên vẹn cho thông tin. Các giải pháp về bảo mật đối với hệ thống phải đảm bảo hệ thống không bị đánh cắp dữ liệu hay bị phá hoại. Sử dụng các cơ chế phân quyền người sử dụng, cũng như các thiết bị như tường lửa và các thiết bị khác để đảm bảo an toàn cho cổng thông tin và hệ thống.

- Tính mở: Giải pháp đưa ra phải dễ dàng kết nối cũng như tích hợp thêm các giải pháp khác khi cần thiết. Bên cạnh đó tuân thủ các chuẩn mở để kết nối tới những hệ thống khác trong tương lai để trao đổi thông tin cũng như các thao tác khác của người sử dụng.

- Tính linh động: hệ thống cần phải linh động để đáp ứng được các thay đổi dựa trên yêu cầu từ phía người sử dụng cũng như các yêu cầu phát sinh từ hệ thống.

- Tính toàn vẹn: giải pháp phải có các cơ chế sao lưu phục hồi khi hệ thống có lỗi để tránh việc mất mát dữ liệu.

2. Yêu cầu về chức năng chính của Phần mềm Trợ lý ảo hỗ trợ thẩm tra thẩm định (sau đây gọi tắt là Phần mềm trợ lý ảo):

- Quản lý truy cập hệ thống thông tin: Đảm bảo bảo mật thông tin và phân quyền cho người dùng.

- Giao diện tiếng việt, thân thiện với người sử dụng.

- Màn hình Trang chủ (Dashboard): Hiển thị thông tin tổng quan về tình trạng xử lý văn bản, báo cáo thống kê, các thông báo cần chú ý.

- Đồng bộ hóa dữ liệu từ các nền tảng khác: Kết nối với các hệ thống dữ liệu khác để thu thập thông tin cần thiết.

- Quản lý các Tham số (Setting): Cho phép người dùng tùy chỉnh các tham số và quy tắc cho phù hợp với nhu cầu sử dụng.

- Cơ chế vận hành nội bộ nhóm:

+ Giao tiếp trên ứng dụng;

+ Giao tiếp với AI;

+ Quản lý công việc và lịch trình.

- Chức năng lõi (AI): Hỗ trợ chuyên viên trong việc xử lý văn bản

+ Tiếp nhận văn bản từ nhiều nguồn: Scan, ứng dụng sẵn có khác, …

+ Tóm tắt nội dung: Tự động tóm tắt nội dung văn bản, trích xuất thông tin chính, phân loại văn bản.

+ Trích xuất thông tin: Trích xuất thông tin từ văn bản, bao gồm các thông tư, nghị quyết, luật liên quan.

+ Rà soát cơ sở pháp lý.

+ Tổng hợp thông tin: Tổng hợp nội dung văn bản theo các mục như cơ sở phương pháp luận, cơ sở thực tiễn và pháp lý, các ý lớn quan trọng, đánh giá mức độ thực tiễn.

+ Hỗ trợ chuyên viên: Cung cấp công cụ hỗ trợ chuyên viên trong việc phân tích, đánh giá và đưa ra quyết định.

- Báo cáo và phân tích: Thống kê, phân tích và tạo báo cáo về tình trạng xử lý văn bản, hiệu quả công tác thẩm định.

3. Yêu cầu công nghệ:

Phần mềm Trợ lý ảo được áp dụng các công nghệ trí tuệ nhân tạo/học máy tiên tiến nhất như sau:

a) Công nghệ xử lý ngôn ngữ tự nhiên (Natural language processing - NLP)

Công nghệ NLP cho phép nhận dạng tự động các nội dung các bài viết/văn bản có ngôn ngữ tiếng Việt: Xử lý mạng từ liên kết, ngữ nghĩa, ngữ cảnh văn bản để

phân loại các bài viết theo từng chuyên mục, chủ đề cụ thể giúp dễ dàng quan sát và đánh giá nội dung.

b) Công nghệ mô hình ngôn ngữ lớn (Large languague model - LLM)

Công nghệ mới nhất hiện nay cho phép sinh ra câu trả lời tự nhiên từ các kết quả đã tìm kiếm được, trích dẫn đến các nguồn dữ liệu gốc giúp khách hàng xác thực nội dung cũng như tìm hiểu chi tiết hơn.

Ưu điểm nổi bật của Trợ lý ảo áp dụng công nghệ LLM:

- Câu trả lời tự nhiên, đa dạng;

- Có khả năng hiểu ngữ cảnh;

- Cho phép hỏi các nội dung chi tiết trong tài liệu, quy trình, quy định, công văn, thông tư, ...

- Cho phép hỏi đa chiều;

- Có khả năng gợi ý các nội dung liên quan;

- Nạp dữ liệu nhanh hơn.

4. Yêu cầu mô hình triển khai:

- Hệ thống thông tin được thiết kế có khả năng tương thích cao, chịu tải tốt, tốc độ cập nhật nhanh chóng, hỗ trợ đa nền tảng và dễ dàng mở rộng.

** Ứng dụng công nghệ điện toán đám mây:*

- Người dùng cuối không phải cài đặt chương trình ứng dụng trên máy tính.

- Ứng dụng được quản lý thông qua sử dụng trình duyệt web.

- Hệ thống hỗ trợ sử dụng trên các thiết bị di động, máy tính bảng, … (có kết nối Internet).

- Có hệ thống sao lưu dự phòng, dữ liệu được sao lưu định kỳ, đảm bảo tính an toàn cho dữ liệu

5. Yêu cầu đảm bảo bảo mật, an toàn thông tin:

a) Quản lý xác thực thông tin định danh

- Tên đăng nhập phải là duy nhất, không phân biệt hoa thường, chỉ nên chứa tập các ký tự là chữ cái, chữ số, dấu gạch dưới.

- Thiết lập chính sách mật khẩu mạnh:

- Có chức năng reset/ quên mật khẩu:

b) Xử lý xác thực

- Trả về thông báo chung cho trường hợp người dùng đăng ký thông tin định danh (username, email, …) đã tồn tại chức năng đăng ký, hoặc gửi sai thông tin định danh tại các chức năng đăng nhập, reset/quên mật khẩu, đổi địa chỉ email, …

- Bật cơ chế bảo vệ bằng Captcha hoặc các hình thức tương đương khi đăng nhập sai quá 5 lần liên tiếp.

c) Quản lý phiên đăng nhập

- Session phải được quản lý bởi server, sinh ngẫu nhiên và độ dài tối thiểu là 128-bit.

- Session phải được thiết lập thời gian timeout, giá trị timeout nên cân bằng giữa nhu cầu thương mại và yếu tố bảo mật.

- Tạo mới session sau khi đăng nhập thành công.

- Xóa giá trị sessionid và các dữ liệu gắn với session đó khi người dùng đăng xuất.

- Cấu hình thuộc tính "Secure" đối với các ứng dụng sử dụng HTTPS và "HTTP-Only" cho trường Cookie.

- Đối với các chức năng quan trọng có tương tác với database, ứng với mỗi phiên phải sinh thêm 1 token ngẫu nhiên, và thực hiện kiểm tra tính hợp lệ của token này trước khi xử lý truy vấn từ người dùng

d) Phân quyền

- Kiểm tra phân quyền dựa trên các đối tượng được lưu tại server (ví dụ: tham số lưu trên session server, dữ liệu lưu trên DB, …).

- Phân quyền tối thiểu, chỉ đáp ứng đủ chức năng và tài nguyên cho người dùng/ứng dụng.

- Phía giao diện người dùng: Chỉ hiển thị các thành phần giao diện, đường dẫn, hàm, ... tương ứng với quyền của người dùng.

- Phía server: Kiểm tra quyền tác động của người dùng/ứng dụng trên các hàm và tài nguyên tương ứng trước khi thực hiện bất cứ tác vụ nào tới hệ thống.

- Có tính năng xóa phiên làm việc hiện tại của người dùng hoặc các cơ chế tương đương đối với các trường hợp quyền người dùng bị thay đổi hoặc bị disable bởi người dùng có thẩm quyền.

- Không đặt trang quản trị public internet, trong trường hợp bắt buộc phải đặt public phải giới hạn các IP được phép truy cập hoặc sử dụng cơ chế xác thực đa nhân tố.

6. Yêu cầu sao lưu và phục hồi dữ liệu:

Phần mềm Trợ lý ảo cung cấp cơ chế sao lưu dữ liệu an toàn, đảm bảo tính sẵn sàng, toàn vẹn của dữ liệu như sau:

- Kiến trúc nhiều node data dự phòng: Triển khai các node dự phòng theo mô hình Clustering, dữ liệu được đồng bộ giữa các node với nhau.

- Lưu bản sao lưu offline: Hệ thống có thể hỗ trợ tạo job sao lưu/tải dữ liệu định kỳ hoặc đột xuất để sao lưu dữ liệu Database ra lưu tại Site chính và Site dự phòng.