

Một số nguyên tắc chung sử dụng chatbot AI phục vụ công việc

Bộ Khoa học và Công nghệ vừa ban hành Tài liệu hướng dẫn một số nguyên tắc chung đối với công chức, viên chức và người lao động trong cơ quan nhà nước sử dụng các mô hình ngôn ngữ lớn (chatbot AI) phục vụ công việc (Công văn số 557/BKHCN-CĐSQG ngày 31/03/2025). Mục đích của tài liệu này nhằm đưa ra các nguyên tắc chung, dễ hiểu để công chức, viên chức và người lao động trong các cơ quan nhà nước sử dụng chatbot AI hỗ trợ công việc một cách hiệu quả và an toàn.



Công văn số 557/BKHCN-CĐSQG nêu rõ, các cơ quan, đơn vị nếu có nhu cầu áp dụng chatbot AI trong công việc được khuyến khích chủ động tìm hiểu và sử dụng Tài liệu này để triển khai, phổ biến trong tổ chức của mình sao cho phù hợp với thực tế. Tài liệu giúp đảm bảo việc ứng dụng AI diễn ra an toàn và mang lại lợi ích thiết thực.

Nguyên tắc chung

Tuân thủ pháp luật Việt Nam, đảm bảo tôn trọng đầy đủ quyền và lợi ích hợp pháp của cá nhân, tổ chức; Hành vi và cách ứng xử khi sử dụng chatbot AI trong xử lý công việc cần phù hợp với các giá trị đạo đức, văn hóa và truyền thống tốt đẹp của dân tộc Việt Nam; Thực hiện đúng các quy định, hướng dẫn về bảo vệ an ninh mạng và đảm bảo an toàn thông tin mạng theo các quy định pháp luật hiện hành; Chịu trách nhiệm đối với hành vi, cách ứng xử khi sử dụng chatbot AI nhằm phục vụ người dân và doanh nghiệp; đồng thời phối hợp chặt chẽ với các cơ quan chức năng để xử lý kịp thời các hành vi hoặc nội dung thông tin vi phạm pháp luật; Các cơ quan, đơn vị sử dụng chatbot AI có trách nhiệm cung cấp thông tin cơ bản về hệ thống, bao gồm các tình huống tiềm ẩn rủi ro cao, gửi về Bộ Khoa học Công nghệ (Cục Chuyển đổi số quốc gia) để tổng hợp thông qua cổng hỗ trợ trực tuyến; Các nguyên tắc nêu trong tài liệu này không áp dụng đối với việc sử dụng chatbot AI trong các hoạt động nghiên cứu, thực thi công vụ thuộc lĩnh vực quốc phòng, an ninh.

Nguyên tắc trong cung cấp dữ liệu và sử dụng chatbot AI

Một là, không chia sẻ lên chatbot AI bất kỳ dữ liệu, tài liệu nào thuộc danh mục bí mật Nhà nước, cũng như các thông tin nhạy cảm như thông tin cá nhân, tài liệu nội bộ hoặc dữ liệu có thể gây ảnh hưởng đến an ninh, tổ chức.

Hai là, đảm bảo rằng dữ liệu hoặc thông tin cung cấp cho chatbot AI không đi ngược lại truyền thống lịch sử, văn hóa, đạo đức, địa lý, quan điểm chính trị, chủ quyền lãnh thổ, hoặc thuần phong mỹ tục của Việt Nam. Đồng thời, không sử dụng nội dung vi phạm bản quyền, quyền sở hữu trí tuệ hoặc các quyền liên quan khác.

Ba là, khi sử dụng chatbot AI, tránh tạo tài khoản sử dụng tên hoặc mật khẩu trùng với tài khoản công vụ (tài khoản email cơ quan, hệ thống nội bộ...) để đảm bảo an toàn thông tin.

Bốn là, sử dụng chatbot AI một cách thận trọng, hiệu quả và có trách nhiệm.

Năm là, kiểm tra và đánh giá kỹ lưỡng kết quả do chatbot AI cung cấp trước khi sử dụng. Đảm bảo thông tin chính xác, phù hợp với ngữ cảnh công việc và không gây hiểu lầm hoặc sai sót khi áp dụng.

Sáu là, không phụ thuộc hoàn toàn vào chatbot AI, cần kết hợp với kiến thức và kinh nghiệm cá nhân để đưa ra quyết định.

Nguyên tắc sử dụng chatbot AI đối với cơ quan, đơn vị

Một là, tuyên truyền, phổ biến, hướng dẫn cán bộ, công chức, viên chức, người lao động sử dụng chatbot AI phù hợp với chức năng, nhiệm vụ, quyền hạn và đặc thù của cơ quan, đơn vị. Trong đó chú trọng đến việc bảo đảm an toàn, an ninh mạng. Trách nhiệm sử dụng chatbot AI thuộc về người đứng đầu của cơ quan, tổ chức.

Hai là, có trách nhiệm quản lý, bảo mật tài khoản sử dụng chatbot AI; trong trường hợp tài khoản cơ quan, đơn vị bị mất quyền kiểm soát hoặc bị giả mạo, cơ quan, đơn vị phải thông báo tới đơn vị triển khai chatbot AI để kịp thời xử lý.

Ba là, quản lý và phân quyền truy cập trong chatbot AI phải phù hợp với chức năng, nhiệm vụ, quyền hạn của người tham gia sử dụng chatbot AI.

Bốn là, khi cán bộ, công chức, viên chức đã nghỉ việc hoặc chuyển công tác, cơ quan, đơn vị phải thực hiện việc thu hồi khóa bảo mật (nếu có) hoặc hủy tài khoản người dùng chatbot AI nhằm đảm bảo tính bảo mật và quản lý chặt chẽ.

Năm là, từng bước hình thành cơ sở dữ liệu tri thức của riêng mình, từ đó thiết lập chatbot chuyên ngành nhằm phục vụ hoạt động của cơ quan, đơn vị mình.

Sáu là, thường xuyên theo dõi, kịp thời nắm bắt tình hình sử dụng chatbot AI của cán bộ, công chức, viên chức, người lao động thuộc phạm vi quản lý.

Bảy là, đơn vị triển khai chatbot AI có trách nhiệm cung cấp tài liệu hướng dẫn chi tiết và hỗ trợ kỹ thuật thường xuyên để đảm bảo quá trình sử dụng diễn ra thuận lợi và an toàn.

Nguyên tắc sử dụng chatbot AI đối với cán bộ, công chức, viên chức, người lao động

Một là, tự quản lý và chịu trách nhiệm về việc bảo vệ thông tin cá nhân đã khai báo trên các nền tảng, hệ thống thông tin của cơ quan, đơn vị; không được tiết lộ tài khoản đăng nhập hoặc thực hiện kết nối trái phép các nền tảng, hệ thống thông tin của cơ quan, đơn vị vào chatbot AI.

Hai là, khi khai thác, sử dụng chatbot nói chung và chatbot AI nói riêng tại các điểm truy cập Internet công cộng, tuyệt đối không bật chế độ lưu trữ mật khẩu trong quá trình sử dụng.

Ba là, không cung cấp dữ liệu cá nhân, thông tin nhân thân và các thông tin nhạy cảm khác của bản thân hoặc của người khác lên chatbot AI.

Bốn là, không sử dụng chatbot nói chung và chatbot AI nói riêng cho các mục đích trái pháp luật, vi phạm thuần phong mỹ tục, hoặc các hành vi như hacking, tạo deep-fake, lừa đảo.

VVH

Nguồn: TẠP CHÍ KHOA HỌC VÀ CÔNG NGHỆ VIỆT NAM