

UBND TỈNH LAI CHÂU
SỞ KHOA HỌC VÀ CÔNG NGHỆ

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: /SKHCN-BCVTCNTT
V/v hướng dẫn quản lý, khai thác và
sử dụng Trí tuệ nhân tạo (AI) trong
hoạt động công vụ của các cơ quan
hành chính nhà nước tỉnh Lai Châu

Lai Châu, ngày tháng 7 năm 2026

Kính gửi:

- Các sở, ban, ngành, đoàn thể tỉnh;
- UBND các xã, phường.

Thực hiện Kế hoạch số 01-KH/BCĐTW ngày 21/3/2025 của Ban Chỉ đạo Trung ương về Phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số về triển khai Phong trào “Bình dân học vụ số”; Công văn số 6121/UBND-VX ngày 20/7/2026 điều chỉnh, bổ sung Kế hoạch số 2408/KH-UBND ngày 28/5/2025 của UBND tỉnh Lai Châu về nội dung giao Sở Khoa học và Công nghệ chủ trì, hướng dẫn việc triển khai ứng dụng AI trong hoạt động công vụ trên địa bàn tỉnh.

Qua nghiên cứu các quy định hiện hành, Sở Khoa học và Công nghệ ban hành hướng dẫn quản lý, khai thác và sử dụng Trí tuệ nhân tạo (AI) trong hoạt động công vụ của các cơ quan hành chính nhà nước tỉnh Lai Châu theo **Hướng dẫn và các Phụ lục kèm theo.**

Sở Khoa học và Công nghệ kính đề nghị các sở, ban, ngành, đoàn thể tỉnh; UBND các xã, phường, nghiên cứu, triển khai thực hiện./.

Nơi nhận:

- Như trên;
- UBND tỉnh (b/c);
- Giám đốc Sở (b/c);
- Các phòng chuyên môn, đơn vị thuộc Sở (t/h);
- Trang TTĐT Sở;
- Lưu: VT, BCVTCNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Phạm Quang Cường

HƯỚNG DẪN QUẢN LÝ, KHAI THÁC VÀ SỬ DỤNG TRÍ TUỆ NHÂN TẠO (AI) TRONG HOẠT ĐỘNG CÔNG VỤ CỦA CÁC CƠ QUAN HÀNH CHÍNH NHÀ NƯỚC TỈNH LAI CHÂU

(Kèm theo Công văn số /SKHCN-BCVTCNTT ngày tháng năm 2026 của Sở Khoa học và Công nghệ)

I. CĂN CỨ PHÁP LÝ

Luật Trí tuệ nhân tạo (Luật số 134/2025/QH15 ngày 10/12/2025 và có hiệu lực áp dụng từ ngày 01/03/2026);

Luật An ninh mạng (Luật số 116/2025/QH15 ngày 10/12/2025 và có hiệu lực áp dụng từ ngày 01/07/2026);

Luật dữ liệu (Luật số 60/2024/QH15 ngày 30/11/2024 và có hiệu lực áp dụng từ ngày 01/7/2025);

Luật bảo vệ dữ liệu cá nhân (Luật số 91/2025/QH15 ngày 26/6/2025 và có hiệu lực áp dụng từ ngày 01/01/2026);

Luật bảo vệ bí mật Nhà nước (Luật số 117/2025/QH15 ngày 10/12/2025 và có hiệu lực áp dụng từ ngày 01/03/2026);

Luật Sở hữu trí tuệ (Luật số 131/2025/QH15 ngày 10/12/2025 và có hiệu lực áp dụng từ ngày 01/04/2026)

Luật Chuyển đổi số (Luật số 148/2025/QH15 ngày 11/12/2025 và có hiệu lực áp dụng từ ngày 01/07/2026);

Nghị định số 142/2026/NĐ-CP ngày 30 tháng 4 năm 2026 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Trí tuệ nhân tạo;

Quyết định số 2847/QĐ-BKHCN ngày 19/6/2026 của Bộ trưởng Bộ Khoa học và Công nghệ ban hành bộ tiêu chí đánh giá nền tảng trí tuệ nhân tạo hỗ trợ công vụ ở phạm vi quốc gia;

Công văn số 2766/BKHCN-TTCNTT ngày 29/4/2026 về hướng dẫn ứng dụng công nghệ số, trí tuệ nhân tạo hỗ trợ rà soát hệ thống VBQPPL;

Công văn số 557/BKHCN-CĐSQG ngày 31/3/2025 của Bộ Khoa học và Công nghệ 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.

II. MỤC ĐÍCH, YÊU CẦU

1. Mục đích:

- Phổ biến kiến thức, nâng cao nhận thức và kỹ năng quản lý, khai thác và

sử dụng Trí tuệ nhân tạo (AI) cho đội ngũ cán bộ, công chức, viên chức trong hoạt động công vụ của các cơ quan hành chính nhà nước tỉnh Lai Châu, bảo đảm tuân thủ pháp luật về dữ liệu, an ninh mạng, bảo vệ dữ liệu cá nhân, bảo vệ bí mật nhà nước và sở hữu trí tuệ; coi đây là công cụ hữu hiệu để nâng cao năng suất, chất lượng, hiệu quả công tác tham mưu, chỉ đạo, điều hành và phục vụ nhân dân.

- Chuẩn hóa phương pháp làm việc với AI, hình thành thói quen làm việc trên môi trường số, góp phần tích cực vào công cuộc cải cách hành chính, xây dựng chính quyền số, cơ quan chuyên nghiệp, hiện đại, hoạt động hiệu lực, hiệu quả.

- Hình thành môi trường ứng dụng AI an toàn, minh bạch, có trách nhiệm, lấy con người làm trung tâm; bảo đảm AI là công cụ hỗ trợ hoạt động công vụ, không thay thế thẩm quyền, trách nhiệm và quyết định của cán bộ, công chức, viên chức.

2. Yêu cầu:

- Việc sử dụng AI phải tuân thủ nghiêm ngặt các quy định của Đảng, pháp luật của Nhà nước, đặc biệt là Luật trí tuệ nhân tạo, các quy định về bảo vệ bí mật nhà nước, an ninh mạng và bảo vệ dữ liệu cá nhân.

- Con người là trung tâm: AI chỉ là công cụ hỗ trợ; không thay thế thẩm quyền và trách nhiệm quyết định của cán bộ, công chức, viên chức (**Điều 4, Luật Trí tuệ nhân tạo số 134/2025/QH15**).

- Kiểm chứng thông tin: Mọi thông tin, sản phẩm do AI tạo ra phải được cán bộ, công chức, viên chức kiểm chứng, thẩm định, chỉnh sửa và chịu trách nhiệm hoàn toàn về nội dung trước khi sử dụng hoặc ban hành. Tuyệt đối không lạm dụng, phụ thuộc vào AI.

- Ưu tiên sử dụng các nền tảng, giải pháp AI do Việt Nam phát triển và làm chủ (Make in Viet Nam) khi xử lý các dữ liệu mang tính nội bộ, nhạy cảm nhằm đảm bảo an toàn, an ninh và chủ quyền dữ liệu quốc gia. Việc lựa chọn, khai thác và sử dụng các nền tảng AI phục vụ hoạt động công vụ phải ưu tiên các nền tảng đáp ứng Bộ tiêu chí đánh giá nền tảng trí tuệ nhân tạo hỗ trợ công vụ ở phạm vi quốc gia ban hành kèm theo Quyết định số 2847/QĐ-BKHCN ngày 19/6/2026 của Bộ trưởng Bộ Khoa học và Công nghệ, bảo đảm yêu cầu về an toàn thông tin, an ninh mạng, bảo vệ dữ liệu, khả năng kiểm soát, lưu vết và trách nhiệm giải trình.

3. Các hành vi nghiêm cấm (Theo Điều 7, Luật Trí tuệ nhân tạo)

“ 1. Lợi dụng, chiếm đoạt hệ thống trí tuệ nhân tạo để thực hiện hành vi vi phạm pháp luật, xâm phạm quyền, lợi ích hợp pháp của tổ chức, cá nhân.

2. Phát triển, cung cấp, triển khai hoặc sử dụng các hệ thống trí tuệ nhân tạo nhằm mục đích sau đây:

- a) Thực hiện các hành vi bị nghiêm cấm theo quy định của luật;
- b) Sử dụng yếu tố giả mạo hoặc mô phỏng người, sự kiện thật để lừa dối hoặc thao túng nhận thức, hành vi của con người một cách có chủ đích và có hệ thống, gây tổn hại nghiêm trọng đến quyền, lợi ích hợp pháp của con người;
- c) Lợi dụng điểm yếu của nhóm người dễ bị tổn thương, bao gồm trẻ em, người cao tuổi, người khuyết tật, người dân tộc thiểu số hoặc người mất năng lực hành vi dân sự, người bị hạn chế năng lực hành vi dân sự, người có khó khăn trong nhận thức, làm chủ hành vi để gây tổn hại cho chính họ hoặc người khác;

d) Tạo ra hoặc phổ biến nội dung giả mạo có khả năng gây nguy hại nghiêm trọng đến an ninh quốc gia, trật tự, an toàn xã hội.

3. Thu thập, xử lý hoặc sử dụng dữ liệu để phát triển, huấn luyện, kiểm thử hoặc vận hành hệ thống trí tuệ nhân tạo trái với quy định của pháp luật về dữ liệu, bảo vệ dữ liệu cá nhân, sở hữu trí tuệ và an ninh mạng.

4. Cản trở, vô hiệu hóa hoặc làm sai lệch cơ chế giám sát, can thiệp và kiểm soát của con người đối với hệ thống trí tuệ nhân tạo theo quy định của Luật này.

5. Che giấu thông tin bắt buộc phải công khai, minh bạch hoặc giải trình; tẩy xóa, làm sai lệch các thông tin, nhãn, cảnh báo bắt buộc trong hoạt động trí tuệ nhân tạo.

6. Lợi dụng hoạt động nghiên cứu, thử nghiệm, đánh giá hoặc kiểm định hệ thống trí tuệ nhân tạo để thực hiện hành vi trái quy định của luật.”

4. Ứng dụng trí tuệ nhân tạo (AI) trong các ngành, lĩnh vực (Theo Điều 6 Luật Trí tuệ nhân tạo)

“1. Việc ứng dụng trí tuệ nhân tạo trong các ngành, lĩnh vực phải tuân thủ nguyên tắc quản lý rủi ro theo quy định của Luật này và phù hợp với pháp luật có liên quan.

2. Đối với các lĩnh vực thiết yếu có tác động trực tiếp đến tính mạng, sức khỏe, quyền và lợi ích hợp pháp của con người hoặc trật tự, an toàn xã hội, việc ứng dụng trí tuệ nhân tạo phải được quản lý rủi ro ở mức độ chặt chẽ hơn, phù hợp với đặc thù của từng lĩnh vực, trong đó bao gồm một số lĩnh vực sau đây:

a) Lĩnh vực y tế: bảo đảm an toàn cho người bệnh; độ tin cậy trong điều kiện sử dụng thực tế; bảo vệ dữ liệu về sức khỏe theo quy định của pháp luật.

b) Lĩnh vực giáo dục: bảo đảm phù hợp với đặc điểm lứa tuổi và sự phát triển của người học; phòng ngừa rủi ro trong đánh giá, phân loại và tác động đến người học; bảo đảm an toàn dữ liệu và quyền riêng tư.

3. Việc ứng dụng trí tuệ nhân tạo trong hoạt động nghiên cứu khoa học phải bảo đảm tuân thủ đạo đức nghiên cứu, liêm chính khoa học và phòng ngừa hành vi gian lận, đạo văn trong quá trình nghiên cứu và công bố kết quả.

4. Chính phủ, Bộ, cơ quan ngang Bộ trong phạm vi chức năng, nhiệm vụ và quyền hạn của mình quy định chi tiết yêu cầu về an toàn, quản lý rủi ro và điều kiện triển khai đối với việc ứng dụng trí tuệ nhân tạo trong ngành, lĩnh vực quản lý, bảo đảm phù hợp với quy định của Luật này.

III. TỔNG QUAN VỀ TRÍ TUỆ NHÂN TẠO (AI)

1. Một số khái niệm:

- Chuyển đổi số: là quá trình chuyển đổi phương thức hoạt động, quản trị và cung cấp dịch vụ dựa trên công nghệ số, dữ liệu số, hệ thống số, nền tảng số, quy trình số nhằm tạo ra giá trị mới, hiệu quả và minh bạch. (Luật Chuyển đổi số)

- Trí tuệ nhân tạo (AI): là việc thực hiện bằng điện tử các năng lực trí tuệ của con người, bao gồm học tập, suy luận, nhận thức, phán đoán và hiểu ngôn ngữ tự nhiên. (Luật Trí tuệ nhân tạo)

Ví dụ: Phần mềm tự động nhận diện và trích xuất chữ viết từ một văn bản được chụp ảnh (công nghệ OCR) là một ứng dụng của AI.

2. Một số xu hướng AI nổi bật:

Công nghệ AI đang phát triển theo nhiều hướng song hành, tác động trực tiếp đến khả năng ứng dụng trong khu vực công. Một số xu hướng chính bao gồm:

- Mô hình ngôn ngữ lớn (LLM): là một dạng AI chuyên sâu về ngôn ngữ, được huấn luyện trên khối lượng dữ liệu văn bản khổng lồ, có khả năng hiểu và tạo ra ngôn ngữ tự nhiên của con người. Các công cụ chatbot phổ biến hiện nay như ChatGPT hay Gemini là các LLM, có thể trò chuyện, trả lời câu hỏi, viết văn bản một cách linh hoạt.

- AI tổng quát (Artificial general Intelligence – AGI): là một hệ thống AI giả định sở hữu khả năng nhận thức, học hỏi và thực hiện bất kỳ nhiệm vụ trí tuệ nào ở mức độ tương đương hoặc vượt trội con người. Có khả năng thực hiện bất kỳ nhiệm vụ trí tuệ nào mà con người có thể thực hiện.

- AI tạo sinh (Generative AI): Là một nhánh của AI có khả năng tạo ra nội

dung mới hoàn toàn (văn bản, hình ảnh, âm thanh, video) dựa trên dữ liệu đã học, thay vì chỉ phân tích hay phân loại dữ liệu có sẵn. Các LLM là một dạng của AI tạo sinh.

Ví dụ: Yêu cầu AI vẽ một bức tranh theo mô tả hoặc soạn một bài phát biểu mới cho một sự kiện sắp tới.

- AI Agent (tác nhân trí tuệ nhân tạo): là một hệ thống phần mềm thông minh có khả năng tự suy luận, lập kế hoạch và chủ động thực hiện các hành động độc lập để đạt được mục tiêu cụ thể do con người đặt ra.

- Agentic AI: là một hệ thống tiên tiến hơn, có khả năng tự lập kế hoạch đa bước, tự động gọi các công cụ (như API, trình duyệt) và điều phối nhiều AI Agent để giải quyết các vấn đề phức tạp. Đây là bước phát triển tiếp theo, chuyển dịch từ mô hình “Hỏi - Đáp” thụ động (như ChatGPT hiện tại) sang mô hình “Giao nhiệm vụ - Thực hiện” chủ động. Khác với AI tạo sinh chỉ dừng lại ở việc tạo ra nội dung, Agentic AI có khả năng tự nhận thức mục tiêu, tự lập kế hoạch và tự động phối hợp chuỗi các công cụ khác nhau (như tự tra cứu văn bản quy phạm pháp luật, trích xuất dữ liệu, soạn thảo, gửi email và kiểm lỗi) để giải quyết trọn vẹn một quy trình nghiệp vụ phức tạp mà không cần con người can thiệp vào từng bước nhỏ.

- Multimodal AI (Trí tuệ nhân tạo đa thể thức): được thiết kế để xử lý nhiều loại dữ liệu đầu vào cùng lúc, giống như con người. Điều này cho phép tương tác tự nhiên hơn và nâng cao khả năng giải quyết vấn đề trong nhiều lĩnh vực khác nhau.

- Conversational AI (Trí tuệ nhân tạo hội thoại): là công nghệ ứng dụng trí tuệ nhân tạo để mô phỏng các cuộc trò chuyện giống như con người. Hệ thống sử dụng văn bản hoặc giọng nói để hiểu, xử lý và phản hồi ngôn ngữ tự nhiên một cách thông minh và linh hoạt. Bao gồm các chatbot và trợ lý ảo có khả năng xử lý ngôn ngữ tự nhiên.

- AI giải thích được (Explainable AI-XAI): Tập trung vào việc làm cho các mô hình AI trở nên minh bạch, cho phép con người hiểu rõ lý do đằng sau các quyết định hoặc dự đoán của máy, điều này rất quan trọng đối với trách nhiệm giải trình.

- AI xanh (Green AI): Xu hướng tối ưu hóa các mô hình AI để tiêu thụ ít năng lượng và tài nguyên tính toán hơn, hướng tới sự phát triển bền vững.

- AI đạo đức (Ethical AI): Đảm bảo tính công bằng, minh bạch và trách nhiệm giải trình trong các ứng dụng AI.

- Hội tụ công nghệ: AI ngày càng được kết hợp sâu rộng với các công

nghe khác như Internet vạn vật (IoT), Blockchain (để tăng cường bảo mật và tin cậy) và mạng 5G (để xử lý dữ liệu tốc độ cao), tạo ra các hệ thống thông minh và phức tạp hơn.

3. Các công cụ AI phổ biến và tiêu chí lựa chọn

3.1. Phân loại các nhóm công cụ AI phổ biến

- Nhóm 1: Trợ lý ngôn ngữ đa năng (LLMs): Các chatbot có khả năng hỏi - đáp, soạn thảo, tóm tắt, dịch thuật, lên ý tưởng.

Ví dụ: ChatGPT (OpenAI), Gemini (Google), Microsoft Copilot, Claude, Grok, Perplexity AI.

Lưu ý: Đây là các nền tảng công cộng quốc tế, cần hết sức cẩn trọng về bảo mật dữ liệu khi sử dụng.

- Nhóm 2: AI tích hợp trong bộ công cụ văn phòng: Các trợ lý ảo được tích hợp sẵn trong các phần mềm soạn thảo văn bản, bảng tính, trình chiếu, email.

Ví dụ: Microsoft 365 Copilot, Gemini for Google Workspace

Lợi ích: Tăng tốc công việc ngay trên các phần mềm quen thuộc, giảm thời gian chuyển đổi giữa các ứng dụng.

- Nhóm 3: AI chuyên dụng: Các công cụ được thiết kế cho các nhiệm vụ cụ thể.

+ Tổng hợp, xử lý văn bản: NotebookLM (Tổng hợp dữ liệu từ các nguồn được đưa ra, có thể sử dụng để làm tài liệu nghiên cứu, so sánh văn bản).

+ Dịch thuật: Google Translate, DeepL, Microsoft Translator, Zalo AI Dịch (tính năng “Dịch AI” tích hợp trong hệ sinh thái Zalo).

+ Xử lý giọng nói:

Chuyển giọng nói thành văn bản (Speech-to-Text): Whisper AI, FPT.AI Speech-to-Text, VAIS (Vietnam AI Solution), Viettel AI Speech-to-Text, VNPT SmartVoice Speech-to-Text.

Chuyển văn bản thành giọng nói (Text-to-Speech): PlayHT, Vbee AI Voice, FPT.AI Text-to-Speech, Viettel AI Text-to-Speech, VNPT SmartVoice Text-to-Speech.

+ Thiết kế hình ảnh, video: Tạo ảnh, infographic, video ngắn phục vụ công tác tuyên truyền với các công cụ như: Canva (có tính năng Canva AI), Adobe Express/Adobe Firefly, Midjourney, DALL-E, Runway (AI video generator), Pika.

- + Kiểm tra ngữ pháp, diễn đạt: Grammarly, QuillBot, LanguageTool.
- + Tạo Slide tự động: Gamma, Presentation.AI (Tạo Slide tự động, nhanh chóng từ nội dung nhập vào).
- + Tạo sơ đồ tư duy, tóm tắt văn bản: Mapify (cho phép tóm tắt tài liệu bất kỳ thành sơ đồ tư duy với nhiều ngôn ngữ khác nhau).

* Khuyến nghị chung: Khuyến khích ưu tiên lựa chọn các nền tảng AI do doanh nghiệp Việt Nam phát triển (*Make in Vietnam - sử dụng mô hình ngôn ngữ lớn tiếng Việt trong nước do doanh nghiệp Việt Nam làm chủ công nghệ, hạ tầng huấn luyện, suy luận và cung cấp dịch vụ tại Việt Nam*) hoặc các nền tảng AI đáp ứng Bộ tiêu chí đánh giá nền tảng AI hỗ trợ công vụ ở phạm vi quốc gia (*Quyết định số 2847/QĐ-BKHCN ngày 19/6/2026 của Bộ Trưởng Bộ Khoa học và Công nghệ*); có cơ chế bảo vệ dữ liệu, quản lý truy cập, lưu vết, kiểm soát người dùng, khả năng tích hợp với hệ thống thông tin của cơ quan nhà nước và đáp ứng các yêu cầu về an toàn thông tin theo quy định của pháp luật.

3.2. Giới thiệu các nền tảng AI “Make in Vietnam”

Chủ trương “Make in Vietnam” nhấn mạnh việc các sản phẩm công nghệ phải được sáng tạo, thiết kế và chủ động sản xuất tại Việt Nam; hạ tầng huấn luyện, suy luận và cung cấp dịch vụ tại Việt Nam, nhằm đảm bảo an ninh, chủ quyền công nghệ quốc gia. Các nền tảng AI trong nước là lựa chọn ưu tiên khi xử lý các nghiệp vụ, hoạt động công vụ, như:

- AI Luật (Tập đoàn MISA và Luật Việt Nam): Hỗ trợ hỏi đáp pháp luật và rà soát văn bản phục vụ công vụ trên cơ sở hệ thống VBQPPL hiện hành, bao quát 83 lĩnh vực quản lý nhà nước thuộc 17 Bộ và cơ quan ngang Bộ, dựa trên mô hình ngôn ngữ lớn (LLMs) do Tập đoàn MISA và Luật Việt Nam phát triển (<https://LuatVietnamMISA.aicongvu.gov.vn>).

- C-AI Legal (Tập đoàn CMC): Hệ thống hỗ trợ kiểm tra, rà soát VBQPPL Việt Nam do Tập đoàn CMC phát triển.

- CMC AI/CMC GenAI: Hệ sinh thái và dịch vụ AI của Tập đoàn CMC, cung cấp các giải pháp trợ lý ảo, chatbot, computer vision, nền tảng AI tạo sinh cho doanh nghiệp, tích hợp với hạ tầng điện toán đám mây và dữ liệu dùng riêng của tổ chức.

- MISA AMIS OneAI/MISA One AI: Nền tảng AI hợp nhất “Make in Vietnam” do MISA phát triển, tích hợp nhiều mô hình trí tuệ nhân tạo tiên tiến cùng mô hình tiếng Việt, hỗ trợ cơ quan nhà nước, doanh nghiệp và hộ gia đình trong các nghiệp vụ văn phòng, kế toán, quản trị, học tập; nhấn mạnh yếu tố bảo mật dữ liệu trên hạ tầng đặt tại Việt Nam và trợ lý số (ví dụ MISA AVA) tích

hợp trong các sản phẩm MISA AMIS.

- FPT.AI: Cung cấp hệ sinh thái đa dạng từ chatbot, trợ lý ảo, xử lý giọng nói, nhận dạng ký tự quang học (OCR) đến các giải pháp chuyên biệt theo ngành (tài chính-ngân hàng, viễn thông, hành chính công, chăm sóc khách hàng...).

- Viettel AI: Phát triển các giải pháp xử lý tiếng Việt chuyên sâu như nhận dạng giọng nói, tổng hợp tiếng nói, phân tích quan điểm, nhận dạng hình ảnh và video, phục vụ hiệu quả cho các tác vụ đặc thù của Việt Nam trong lĩnh vực quốc phòng, an ninh, tài chính, dịch vụ công.

- Zalo AI: Tích hợp các tính năng trí tuệ nhân tạo trong hệ sinh thái Zalo, nổi bật với trợ lý ảo Kiki và các mô hình ngôn ngữ tối ưu cho tiếng Việt, hỗ trợ người dùng trong tra cứu thông tin, giải trí, điều khiển thiết bị thông minh, cũng như cung cấp các dịch vụ cho doanh nghiệp.

- VNPT AI: Hệ sinh thái trí tuệ nhân tạo do VNPT phát triển (VNPT AI, VNPT SmartBot, VNPT SmartVision, VNPT SmartVoice, VNPT GenAI...), cung cấp các mô hình nhận dạng tiếng nói, nhận diện khuôn mặt, phân tích hình ảnh, trợ lý ảo, phân tích dư luận số và mô hình ngôn ngữ lớn (LLM) tối ưu cho tiếng Việt, đã được ứng dụng trong nhiều hệ thống dịch vụ công và dịch vụ số.

- Vbee: Nền tảng chuyển văn bản thành giọng nói (Text-to-Speech) tiếng Việt, cung cấp giọng đọc tự nhiên, giàu cảm xúc, hỗ trợ đa vùng miền; được sử dụng trong đọc tin, thuyết minh, tổng đài tự động, nội dung số và một số hệ thống dịch vụ công.

- VAIS (Vietnam AI Solution): Doanh nghiệp AI tập trung vào lõi nhận dạng tiếng nói (Speech-to-Text) và xử lý ngôn ngữ tiếng Việt, triển khai các giải pháp ghi âm – phiên mã, trợ lý ảo và ứng dụng AI giọng nói tại nhiều cơ quan Đảng, Nhà nước và doanh nghiệp.

- Các nền tảng khác: Bên cạnh các nền tảng nêu trên, một số nền tảng AI “Make in Vietnam” khác đang tiếp tục được các doanh nghiệp công nghệ trong nước nghiên cứu, phát triển và hoàn thiện (VMS AI – Trung tâm tri thức hình ảnh và giám sát thông minh; Trợ lý Chatbot hành chính công (*Công ty Cổ phần đầu tư Kỷ nguyên mới Việt Nam*); AI Agent – Trợ lý ảo thủ tục hành chính công (*Công ty Thanh Bình*); Phần mềm quản trị điều hành cấp xã (*Trường Đại học Khoa học Tự nhiên*)... Các cơ quan, đơn vị có thể nghiên cứu, đánh giá, lựa chọn, thử nghiệm và đưa vào danh mục khuyến nghị sử dụng tùy theo yêu cầu nghiệp vụ cụ thể, bảo đảm an toàn, an ninh dữ liệu và hiệu quả chi phí.

IV. KỸ NĂNG SỬ DỤNG AI HIỆU QUẢ VÀ AN TOÀN

1. Kỹ năng đặt yêu cầu (Prompt Engineering)

Chất lượng của kết quả do AI tạo ra phụ thuộc rất lớn vào chất lượng của câu lệnh yêu cầu (prompt). Một câu lệnh hiệu quả cần rõ ràng, cụ thể và cung cấp đủ thông tin cho AI.

- **Nguyên tắc “R-V-N-Đ”**: Một câu lệnh hiệu quả cần có 4 yếu tố: **R**õ ràng (nhiệm vụ cụ thể, yêu cầu hành động cốt lõi), **V**ai trò (chỉ định AI đóng vai trò chuyên gia), **N**gữ cảnh (cung cấp thông tin nền, mô tả tình huống đang diễn ra để AI hiểu không gian dữ liệu), **Đ**ịnh dạng (yêu cầu đầu ra mong muốn, hình thức trình bày mong muốn).

Ví dụ kém hiệu quả: “Viết về cải cách hành chính”.

Ví dụ hiệu quả: “Bạn là một chuyên gia về cải cách hành chính. Hãy soạn một bài phát biểu dài 800 từ cho lãnh đạo, với văn phong trang trọng, về các giải pháp đột phá nhằm nâng cao sự hài lòng của người dân đối với dịch vụ công. Yêu cầu đầu ra có 3 phần chính: Thực trạng, Giải pháp, Kiến nghị”.

- Các kỹ thuật nâng cao (diễn giải đơn giản):

+ *Cung cấp ví dụ*: Đưa ra một vài ví dụ về kết quả mong muốn để AI học theo. *Ví dụ: “Hãy tóm tắt văn bản sau theo 3 gạch đầu dòng, văn phong hành chính. Ví dụ: ‘-Tăng cường kỷ luật, kỷ cương. - Đẩy mạnh ứng dụng CNTT. – Nâng cao trách nhiệm người đứng đầu.’”.*

+ *Yêu cầu suy luận từng bước*: Yêu cầu AI giải thích logic trước khi đưa ra câu trả lời cuối cùng để tăng độ chính xác, đặc biệt với các vấn đề phức tạp. *Ví dụ: “Phân tích ưu và nhược điểm của phương án A và phương án B, sau đó hãy đề xuất lựa chọn phương án tối ưu và giải thích tại sao”.*

2. Tích hợp AI vào quy trình công việc hàng ngày

- Trước khi thực hiện: Dùng AI để lên ý tưởng, xây dựng dàn ý, tìm kiếm thông tin ban đầu, tạo khung sườn cho báo cáo hoặc kế hoạch.

- Trong khi thực hiện: Dùng AI để soạn thảo nội dung thô, tóm tắt các tài liệu tham khảo dài, dịch thuật các văn bản không nhạy cảm, kiểm tra lỗi chính tả và ngữ pháp.

- Sau khi thực hiện: Dùng AI để chuẩn hóa lại văn phong của văn bản, tạo slide trình bày từ nội dung đã có, tạo infographic để tóm tắt các kết quả chính.

3. Quy trình 5 bước kiểm chứng kết quả từ AI

Đây là quy trình bắt buộc phải thực hiện đối với mọi sản phẩm do AI tạo ra trước khi đưa vào sử dụng chính thức:

- Bước 1 – Đánh giá dữ liệu đầu vào: Đây là bước tiên quyết. Cán bộ, công chức, viên chức phải phân loại cấp độ thông tin (công khai, nội bộ, dữ liệu cá nhân hay bí mật nhà nước) trước khi nhập. Dựa trên phân loại này, quyết định có được phép sử dụng AI công cộng hay không, tuân thủ nghiêm ngặt các nguyên tắc bảo mật dữ liệu.

Trường hợp dữ liệu thuộc phạm vi bí mật nhà nước, dữ liệu cá nhân nhạy cảm hoặc dữ liệu thuộc danh mục hạn chế chia sẻ theo quy định của pháp luật thì không được đưa lên các nền tảng AI công cộng; chỉ được xử lý trên hệ thống AI chuyên dùng hoặc nền tảng được cơ quan có thẩm quyền cho phép.

- Bước 2 – Kiểm tra tính chính xác của dữ kiện và đối chiếu với quy định: Đối chiếu mọi số liệu, tên riêng, ngày tháng, sự kiện với nguồn thông tin gốc, đáng tin cậy (văn bản pháp quy, Cổng thông tin điện tử chính thức, số liệu của Tổng cục Thống kê...). Rà soát các nội dung liên quan đến chủ trương, chính sách, quy phạm pháp luật với các văn bản gốc của Đảng và Nhà nước để đảm bảo không có sai lệch hoặc diễn giải sai.

- Bước 3 – Rà soát văn phong và thuật ngữ: Chỉnh sửa câu chữ, thuật ngữ để đảm bảo phù hợp với văn phong hành chính, chính trị; đúng với chuyên ngành và không gây hiểu lầm.

- Bước 4 – Hoàn thiện và chịu trách nhiệm: Cán bộ, công chức, viên chức thực hiện chỉnh sửa cuối cùng, bổ sung quan điểm, nhận định của bản thân, ký nháy hoặc chịu trách nhiệm về sản phẩm cuối cùng theo quy chế làm việc của cơ quan.

- Bước 5 – Dấu vết và minh bạch: Để phục vụ công tác giải trình, cần lưu lại các câu lệnh (prompt) quan trọng, các lần chỉnh sửa lớn và nguồn thông tin đã dùng để kiểm chứng. Đặc biệt, đối với các văn bản, báo cáo hoặc sản phẩm truyền thông được tạo ra với sự hỗ trợ đáng kể từ AI, cán bộ cần thực hiện gán nhãn hoặc chú thích ở cuối tài liệu.

V. KỸ NĂNG VÀ NĂNG LỰC CẦN THIẾT ĐỂ SỬ DỤNG AI

1. Kiến thức nền tảng về AI

- Hiểu các khái niệm cơ bản như Machine Learning, NLP...
- Ứng dụng AI trong hành chính công (trợ lý ảo, phân tích dữ liệu, tự động hóa).
- Nhận thức về giới hạn, rủi ro và đạo đức AI.

2. Kỹ năng phân tích và quản lý dữ liệu

- Thu thập, làm sạch, xử lý dữ liệu hiệu quả.

- Đọc hiểu và phân tích dữ liệu bằng công cụ AI.
- Đảm bảo bảo mật thông tin và tuân thủ quy định về dữ liệu cá nhân.

3. Tư duy phản biện và giải quyết vấn đề

- Xác định vấn đề rõ ràng để AI hỗ trợ hiệu quả.
- Đánh giá và kiểm chứng kết quả AI đưa ra.
- Điều chỉnh yêu cầu để AI cung cấp phản hồi chính xác hơn.

4. Giao tiếp và hợp tác trong môi trường số

- Sử dụng AI để hỗ trợ soạn thảo văn bản, báo cáo, dịch thuật.
- Ứng dụng AI vào các công cụ làm việc nhóm (Google Docs, Microsoft 365).
- Trình bày và giải thích kết quả AI một cách rõ ràng.

5. Đào tạo và phát triển năng lực AI

- Tham gia các chương trình đào tạo AI chính thức cho công chức, viên chức.
- Khuyến khích các đơn vị tổ chức mô hình sinh hoạt chuyên đề “Cùng thực hành AI” để chia sẻ kinh nghiệm và các câu lệnh hiệu quả.
- Xây dựng cộng đồng chia sẻ kiến thức và kinh nghiệm về AI.
- Tự học qua các khóa học trực tuyến, tài liệu nghiên cứu.

6. Ứng dụng AI có trách nhiệm

- Tuân thủ quy định pháp luật, đạo đức khi sử dụng AI.
- Đảm bảo tính minh bạch, công bằng trong các ứng dụng AI.
- Không phụ thuộc hoàn toàn vào AI, luôn có sự kiểm tra của con người.

VI. AN TOÀN, BẢO MẬT VÀ ĐẠO ĐỨC

AI tạo sinh là một “con dao hai lưỡi”. Bên cạnh những lợi ích to lớn, nó cũng tiềm ẩn những rủi ro nghiêm trọng về an toàn thông tin, đặc biệt trong môi trường chính trị. Việc AI tạo ra thông tin sai lệch không chỉ là một lỗi kỹ thuật mà có thể trở thành một vấn đề chính trị, tư tưởng nếu cán bộ, công chức, viên chức thiếu cảnh giác, sử dụng và phổ biến các thông tin này. Điều này có thể dẫn đến vi phạm các quy định của Đảng, pháp luật của Nhà nước, đặc biệt là Luật An ninh mạng.

1. Bảo mật dữ liệu là ưu tiên số một

Cán bộ, công chức, viên chức phải tự hình thành thói quen phân loại mức

độ nhạy cảm của thông tin trước khi tương tác với bất kỳ hệ thống AI nào.

- Cấp độ 1 (Công khai): Thông tin đã được công bố trên các phương tiện thông tin đại chúng, Cổng thông tin điện tử chính thức. *Có thể sử dụng các công cụ AI công cộng để xử lý.*

- Cấp độ 2 (Nội bộ): Thông tin lưu hành trong nội bộ cơ quan, không chứa bí mật nhà nước (Ví dụ: lịch công tác tuần, báo cáo công việc không mật). *Hạn chế sử dụng AI công cộng, ưu tiên các giải pháp AI nội bộ hoặc nền tảng “Make in Vietnam” có cam kết bảo mật.*

- Cấp độ 3 (Dữ liệu cá nhân): Thông tin định danh hoặc gắn với một cá nhân cụ thể (họ tên, ngày sinh, số CCCD, tình trạng sức khỏe, quan điểm chính trị...). Phải tuân thủ nghiêm ngặt Luật bảo vệ dữ liệu cá nhân. Tuyệt đối không đưa lên AI công cộng nếu chưa có sự đồng ý của chủ thể và các biện pháp bảo vệ cần thiết.

- Cấp độ 4 (Bí mật nhà nước): Thông tin thuộc danh mục bí mật nhà nước theo quy định của pháp luật. TUYỆT ĐỐI CẤM đưa vào bất kỳ hệ thống AI nào không được cơ quan có thẩm quyền cấp phép riêng cho việc xử lý tài liệu mật.

2. Kiểm soát kết nối và tích hợp hệ thống

Nghiêm cấm mọi hình thức tự ý kết nối, tích hợp trái phép các hệ thống thông tin nội bộ, hệ thống cơ sở dữ liệu nghiệp vụ của cơ quan vào các nền tảng AI bên ngoài, đặc biệt là các nền tảng AI công cộng không rõ nguồn gốc.

Việc tích hợp (nếu có nhu cầu nghiệp vụ) chỉ được thực hiện khi có phê duyệt của cấp có thẩm quyền, sau khi đã được bộ phận chuyên trách (CNTT, an ninh mạng) tiến hành đánh giá rủi ro an ninh mạng chi tiết, có phương án kỹ thuật bảo vệ và phải ghi nhật ký (log) hệ thống đầy đủ để phục vụ công tác giám sát, kiểm tra.

Mọi hoạt động kết nối API, chia sẻ dữ liệu hoặc tích hợp hệ thống AI với các hệ thống thông tin, cơ sở dữ liệu của cơ quan nhà nước phải được đánh giá tác động về an toàn thông tin, an ninh mạng và bảo vệ dữ liệu trước khi triển khai; đồng thời phải được người có thẩm quyền phê duyệt theo quy định.

3. Nhận diện và phòng tránh các rủi ro từ AI tạo sinh

- Hiện tượng “Ảo giác” (Hallucination): Là tình trạng AI tự bịa đặt thông tin, dữ kiện, số liệu hoặc thậm chí là các vụ việc không có thật nhưng trình bày một cách rất logic và thuyết phục. Đây là một trong những rủi ro lớn nhất, đòi hỏi người dùng phải luôn thực hiện quy trình kiểm chứng.

- Nội dung giả mạo (Deepfake): AI có thể được sử dụng để tạo ra các video, hình ảnh, âm thanh giả mạo (ví dụ: giả mạo giọng nói của Lãnh đạo để đưa ra các chỉ đạo sai lệch hoặc tạo hình ảnh sai sự thật về một sự kiện). Cần nâng cao cảnh giác, luôn xác thực thông tin từ nhiều kênh chính thức trước khi tin và phổ biến.

- Tấn công lừa đảo (Phishing) tinh vi: Kẻ xấu có thể dùng AI để soạn các email, tin nhắn lừa đảo với ngôn ngữ tự nhiên, không sai lỗi chính tả, mạo danh đồng nghiệp, cấp trên để yêu cầu chuyển tiền, cung cấp mật khẩu hoặc thông tin nhạy cảm. Cần hết sức cẩn trọng với các yêu cầu đột xuất, bất thường.

- Lộ lọt thông tin nhạy cảm: Mọi dữ liệu được nhập vào các mô hình AI công cộng đều có thể được nhà cung cấp dịch vụ sử dụng để huấn luyện lại mô hình và có nguy cơ bị truy cập bởi bên thứ ba. Cần ghi nhớ quy tắc vàng: “Đừng nhập vào AI những gì bạn không muốn đăng lên mạng xã hội”.

4. Kỹ năng nhận diện sản phẩm giả mạo (Deepfake)

Cán bộ, công chức, viên chức cần cảnh giác trước các cuộc gọi video hoặc tin nhắn đa phương tiện có dấu hiệu sau:

- Thời lượng ngắn bất thường, chất lượng kết nối chập chờn (cố tình).
- Khuôn mặt thiếu cảm xúc tự nhiên, mắt ít chớp hoặc hướng nhìn không tập trung.
- Màu sắc da và ánh sáng không khớp với bối cảnh phía sau; vùng cổ hoặc viền tóc bị mờ nhòe.
- Âm thanh giọng nói đều đều, thiếu ngữ điệu tự nhiên hoặc khẩu hình miệng không khớp với lời nói.
- Biện pháp xử lý: Chủ động ngắt cuộc gọi và xác thực lại qua kênh liên lạc truyền thống (điện thoại) trước khi thực hiện bất kỳ giao dịch tài chính hay cung cấp thông tin nào.

5. Trách nhiệm của cán bộ, công chức, viên chức và đơn vị quản lý

- Trách nhiệm giải trình: Phải có khả năng giải trình được quá trình sử dụng AI và cách thức kiểm chứng thông tin khi được yêu cầu.
- Quản lý tài khoản: Tuân thủ nghiêm ngặt quy định về quản lý tài khoản và mật khẩu. Tuyệt đối không sử dụng email công vụ để đăng ký các dịch vụ AI cá nhân, các nền tảng không được cơ quan cấp phép. Tuyệt đối không đặt mật khẩu tài khoản AI công cộng (hoặc các dịch vụ cá nhân khác) trùng hoặc tương tự với mật khẩu các hệ thống công vụ (email, hệ thống nội bộ). Phải sử dụng mật khẩu mạnh, có tính phức tạp và thực hiện thay đổi định kỳ theo quy chế của

cơ quan.

Không sử dụng chung tài khoản AI giữa nhiều cá nhân; không chia sẻ khóa truy cập (API Key), mã xác thực hoặc thông tin định danh tài khoản AI cho tổ chức, cá nhân khác khi chưa được phép.

- Minh bạch (khi cần thiết): Trong các tài liệu lưu hành nội bộ, có thể ghi chú “Nội dung có tham khảo, hỗ trợ từ công cụ AI và đã được kiểm chứng” để tăng tính minh bạch và hình thành ý thức chung trong cơ quan, đơn vị.

Khi sử dụng AI để tạo lập tài liệu, hình ảnh, âm thanh hoặc sản phẩm số phục vụ hoạt động công vụ, cán bộ, công chức, viên chức phải kiểm tra nguy cơ vi phạm quyền tác giả, quyền liên quan, quyền sở hữu công nghiệp và các quyền sở hữu trí tuệ khác; không sử dụng AI để tạo lập hoặc phát tán sản phẩm xâm phạm quyền sở hữu trí tuệ của tổ chức, cá nhân.

- Trách nhiệm của đơn vị quản lý (Tổ chức - CNTT): Bộ phận Tổ chức – CNTT (hoặc các đơn vị có chức năng tương đương) của cơ quan chịu trách nhiệm xây dựng và thực thi quy trình thu hồi, khóa hoặc hủy tài khoản (bao gồm tài khoản AI nội bộ và các tài khoản do cơ quan cấp phép) ngay khi cán bộ, công chức, viên chức điều chuyển công tác, nghỉ hưu hoặc nghỉ việc. Quy trình này nhằm đảm bảo an toàn, an ninh thông tin, ngăn chặn truy cập trái phép và thu hồi tài sản số của cơ quan.

Phụ lục I

VÍ DỤ MẪU CÂU LỆNH (FROMPT) CHO CÁC TÁC VỤ HÀNH CHÍNH

(Kèm theo Công văn số /SKHCN-BCVTCNTT ngày tháng năm 2026 của Sở Khoa học và Công nghệ)

1. Prompt dự thảo công văn hành chính

Ví dụ: Đóng vai chuyên viên Văn phòng UBND, hãy soạn thảo một Công văn hành chính với nhiệm vụ đơn đốc các Sở, Ban, Ngành nộp báo cáo về tình hình tuyên truyền phòng chống lụt bão quý 2 năm 2026. Yêu cầu tuân thủ Nghị định số 30/2020/NĐ-CP của Chính phủ về công tác văn thư. Phân chia rõ 3 phần: căn cứ ban hành; nội dung đơn đốc cụ thể; thời hạn hoàn thành và trách nhiệm người đứng đầu. Sử dụng từ ngữ mạch lạc, khách quan, mang tính mệnh lệnh hành chính. Trình bày bản nháp bằng cấu trúc hành chính, bôi đậm các mốc thời gian quan trọng.

2. Prompt dự thảo biên bản cuộc họp

Tôi có một số tài liệu từ một cuộc họp vừa diễn ra, bao gồm các mẫu ghi chú viết tay rời rạc và văn bản chuyển chữ (transcript) từ băng ghi âm. Các tài liệu này hiện tại đang chứa nhiều từ ngữ thừa, văn phong nói và chưa được sắp xếp một cách khoa học. Là một Thư ký cuộc họp chuyên nghiệp và là một chuyên gia xử lý ngôn ngữ tự nhiên (NLP) có khả năng tổng hợp thông tin cực kỳ sắc bén, logic. Hãy chuyển đổi toàn bộ thông tin đầu vào tại phần [Ghi chép và ghi chú cuộc họp vào đây] thành một BIÊN BẢN CUỘC HỌP chính thức. Trong quá trình xử lý, bạn phải tuân thủ nghiêm ngặt các nguyên tắc sau: 1. Trích xuất chính xác các thông tin hành chính cơ bản. 2. Tóm tắt ý kiến phát biểu bằng cách lược bỏ hoàn toàn từ ngữ thừa, văn phong nói mang tính khẩu ngữ. Cô đọng ý chính của từng đại biểu thành các gạch đầu dòng mạch lạc, dễ hiểu, lý luận chính trị và hành chính. 3. Làm nổi bật rõ ràng các chỉ đạo, kết luận và quyết định cuối cùng của Chủ tọa, Chủ trì cuộc họp. Tuyệt đối không bịa đặt thông tin hoặc tự ý thêm bớt các thông tin nằm ngoài văn bản gốc được cung cấp. Xuất kết quả theo cấu trúc chuẩn của một biên bản cuộc họp như mẫu kèm theo [Dán mẫu biên bản cuộc họp vào đây].

3. Prompt tóm tắt văn bản, báo cáo

Tôi có một Báo cáo chuyên đề dài 50 trang chứa rất nhiều thông tin, dữ liệu và số liệu phân tích phức tạp tại phần [Tải lên file dữ liệu]. Do ban lãnh đạo không có nhiều thời gian, tôi cần "nén" toàn bộ tài liệu này thành một bản tóm tắt chiến lược siêu ngắn gọn nhưng vẫn đảm bảo giữ trọn vẹn các nội dung quan trọng. Bạn là một chuyên viên có khả năng lọc thông tin, nắm bắt bản chất vấn

đề cực tốt và tư duy số liệu nhạy bén. Hãy đọc hiểu toàn bộ tài liệu được cung cấp và viết một Bản tóm tắt dành cho Lãnh đạo. Trong quá trình xử lý, bạn phải tuân thủ các yêu cầu sau: 1. Không diễn giải dông dài, sử dụng văn phong trực diện, súc tích và có tính hành động cao. 2. Trích xuất chính xác, trung thực các số liệu định lượng (như ngân sách, % tăng trưởng,...) từ báo cáo gốc mà không tự ý thay đổi hay suy diễn. 3. Ưu tiên cấu trúc thông tin rõ ràng, dễ đọc lướt để người điều hành có thể nắm bắt toàn bộ thông tin trọng tâm chỉ trong 1 phút. Trình bày kết quả gói gọn hoàn toàn trong giới hạn 1 trang A4 chiến lược theo đúng cấu trúc 3 phần sau đây: **BẢN TÓM TẮT DÀNH CHO LÃNH ĐẠO**. Phần 1: Các kết luận quan trọng (Tóm tắt 3 kết luận quan trọng nhất của báo cáo bằng đúng 3 câu đơn cực kỳ súc tích) - Câu 1: [Nội dung kết luận 1] - Câu 2: [Nội dung kết luận 2] - Câu 3: [Nội dung kết luận 3]. Phần 2: Số liệu định lượng chính (Trích xuất toàn bộ các số liệu về ngân sách, % tăng trưởng và các chỉ số tài chính/vận hành quan trọng khác vào bảng dưới đây) | Chỉ tiêu/Hạng mục | Số liệu thực tế / Chỉ số | Ghi chú ngắn | --- | --- | --- |. | [Ví dụ: Ngân sách dự án] | [Số liệu] | [Mục đích/Trạng thái] | | [Ví dụ: Tốc độ tăng trưởng] | [Số liệu %] | [So với cùng kỳ] |. Phần 3: Cảnh báo rủi ro (Liệt kê chính xác 3 rủi ro cốt lõi nhất được cảnh báo trong báo cáo) *Rủi ro 1: [Tên rủi ro] - [Mô tả ngắn gọn hệ quả]; *Rủi ro 2: [Tên rủi ro] - [Mô tả ngắn gọn hệ quả]; *Rủi ro 3: [Tên rủi ro] - [Mô tả ngắn gọn hệ quả].

4. Prompt viết bài truyền thông

4.1. Prompt chuyên nghiệp đăng tải trên Cổng thông tin điện tử tỉnh, Trang Thông tin điện tử của cơ quan hoặc các Tạp chí

Cơ quan tôi vừa ban hành một văn bản Nghị quyết/Báo cáo chính trị quan trọng tại phần [Dán văn bản]. Tuy nhiên, văn bản gốc mang tính chất hành chính, khá khô khan và khó tiếp cận với đại đa số công chúng. Chúng tôi cần biến đổi nội dung này thành một bài viết truyền thông hấp dẫn để đăng tải trên Cổng thông tin điện tử tỉnh, Trang Thông tin điện tử của cơ quan nhằm lan tỏa thông tin một cách rộng rãi. Là một Biên tập viên báo chí/Chuyên viên truyền thông chuyên nghiệp, có kinh nghiệm dày dặn trong việc "bình dân hóa" các văn bản pháp luật, nghị quyết nhưng vẫn giữ vững tính chuẩn mực chính trị. Hãy chuyển đổi nội dung văn bản hành chính phức tạp thành 01 bài/tin truyền thông hoàn chỉnh. Trong quá trình viết, bạn phải tuân thủ các quy tắc sau: 1. Quy tắc báo chí: Áp dụng mô hình "Tháp ngược" - Đưa thông tin quan trọng nhất, các quyết sách nổi bật nhất lên ngay đoạn Sapo đầu bài. 2. Ngôn từ: Gắn gũi, dễ hiểu, có tính lan tỏa cao, nhưng TUYỆT ĐỐI tuân thủ các chuẩn mực chính trị, không dùng từ ngữ tùy tiện làm sai lệch bản chất của văn bản gốc. Vui lòng trình bày bài viết theo đúng cấu trúc tiêu chuẩn của một bài báo điện tử như sau:

[TIÊU ĐỀ CHÍNH]

(Yêu cầu: Thu hút, tạo sự chú ý nhưng phải phản ánh đúng bản chất chính trị của nghị quyết)

[ĐOẠN TÓM TẮT (SAPO)]

(Yêu cầu: Đưa các thông tin quan trọng nhất, quyết sách nổi bật nhất lên đầu)

[THÂN BÀI]

(Yêu cầu: Chia nhỏ nội dung thành các mục có tiêu đề phụ - Sub-heading rõ ràng, mạch lạc)

1. [Tiêu đề phụ 1]

[Nội dung phân tích/diễn giải...]

2. [Tiêu đề phụ 2]

[Nội dung phân tích/diễn giải...]

[DANH SÁCH CÂU TRÍCH DẪN QUAN TRỌNG]

(Yêu cầu: Trích xuất sẵn 3 câu phát biểu hoặc nội dung cốt lõi nhất từ văn bản gốc để tòa soạn bôi đậm/làm nổi bật (Quote) trong bài viết)

- Quote 1: "[Nội dung câu trích dẫn 1]"

- Quote 2: "[Nội dung câu trích dẫn 2]"

- Quote 3: "[Nội dung câu trích dẫn 3]"

4.2. Prompt truyền thông chính sách

- *Prompt 1:* Hãy đóng vai một các nộ chính sách, soạn thảo một bản tóm tắt ngắn gọn (300 từ) về chính sách mới về quản lý nước sạch, tập trung vào các điểm chính và lợi ích cho cộng đồng, giọng điệu trang trọng.

- *Prompt 2:* Hãy đóng vai một cán bộ truyền thông, soạn thảo một bài viết ngắn (250 từ) trên mạng xã hội về chính sách hỗ trợ doanh nghiệp nhỏ và vừa, tập trung vào lợi ích và cách đăng ký, giọng điệu dễ hiểu.

- *Prompt 3:* Hãy phát triển một bản tin nội bộ (400 từ) cho cán bộ về chính sách mới liên quan đến bảo vệ môi trường, bao gồm các thay đổi chính và hướng dẫn thực hiện, giọng điệu chuyên nghiệp.

5. Prompt dự thảo bài phát biểu

Đơn vị của chúng tôi chuẩn bị tổ chức một hội nghị quan trọng về [Chủ đề]. Để khai mạc hội nghị, tôi cần một bài phát biểu mang tính chiến lược nhưng phải khắc phục được điểm yếu thông thường của các bài diễn văn hành chính

(vốn hay bị khô khan, thiếu cảm xúc và mang nặng tính báo cáo số liệu). Đối tượng lắng nghe trực tiếp là toàn thể cán bộ, công chức, viên chức cấp cơ sở. Bạn là Bí thư Cấp uỷ - người đứng đầu tổ chức, đồng thời là một nhà hùng biện xuất sắc, có tầm nhìn chiến lược, khả năng thấu hiểu tâm lý quần chúng và sở hữu phong thái lãnh đạo gần gũi, quyết liệt. Hãy soạn thảo toàn văn bài phát biểu khai mạc hội nghị về [Chủ đề]. Trong quá trình viết, bạn phải tuân thủ nghiêm ngặt các nguyên tắc sau: 1. Đối tượng & Ngôn ngữ: Sử dụng ngôn ngữ gần gũi, thực tiễn, dễ hiểu, phù hợp với tư duy và góc nhìn của cán bộ, đảng viên cấp cơ sở. 2. Âm hưởng (Tone/Voice): Tràn đầy năng lượng, truyền cảm hứng mạnh mẽ, khơi dậy được 'khát vọng vươn lên' và tinh thần 'chung sức đồng lòng' trong tập thể. 3. Tinh thần chính trị: Thẳng thắn, khách quan, "nhìn thẳng vào sự thật, không né tránh" khi nói về tồn tại và nhấn mạnh phương châm "nói đi đôi với làm". Trình bày bài phát biểu theo đúng bố cục bắt buộc dưới đây:

BÀI PHÁT BIỂU KHAI MẠC HỘI NGHỊ VỀ [CHỦ ĐỀ]

(Của Đồng chí Bí thư Cấp uỷ)

1. Phần Mở Đầu: Đặt vấn đề và chào mừng

- [Nội dung: Chào hỏi theo đúng nghi thức, thu hút sự chú ý của hội trường, tạo không khí ấm áp, gần gũi ban đầu và nêu bật lý do của hội nghị].

2. Phần Thân Bài: Nhìn lại và định hướng

- Điểm lại 3 thành tựu: [Nội dung: Tóm tắt nhanh 3 kết quả tự hào nhất một cách sinh động, có cảm xúc thay vì liệt kê số liệu thô].

- Chỉ ra 2 điểm nghẽn cần khắc phục: [Nội dung: Thẳng thắn nêu rõ 2 hạn chế lớn nhất với tinh thần xây dựng, nhìn thẳng vào sự thật, không né tránh].

3. Phần Kết luận: Kêu gọi hành động

- Thông điệp hành động: [Nội dung: Đưa ra lời kêu gọi quyết liệt, nhấn mạnh tinh thần "nói đi đôi với làm", "chung sức đồng lòng", khơi dậy khát vọng cống hiến của từng cán bộ, đảng viên để kết thúc bài phát biểu một cách đầy hào hùng].

Thông tin bổ sung:

- Chủ đề hội nghị: [Điền chủ đề cụ thể của bạn vào đây]

- Một số lưu ý hoặc số liệu đặc biệt (nếu có): [Điền vào đây]

6. Prompt tương tác với công dân

- *Prompt 1:* Hãy đóng vai một cán bộ một cửa/dịch vụ công, soạn thảo văn bản/email trả lời thắc mắc của công dân về thủ tục “Xin cấp phép xây dựng”,

cung cấp hướng dẫn từng bước và thông tin liên hệ, 200 từ, giọng điệu thân thiện.

- *Prompt 2*: Hãy viết thư gửi công dân về mối quan ngại của họ liên quan đến việc thu phí rác thải mới, giải thích lý do và cách tham gia đóng góp ý kiến, 300 từ, giọng điệu trang trọng.

- *Prompt 3*: Hãy đóng vai một cán bộ một cửa/dịch vụ công, soạn thảo hướng dẫn (300 từ) cho công dân về cách sử dụng chatbot chính phủ để tra cứu thông tin hộ khẩu, giọng điệu thân thiện.

7. Prompt Chuyển đổi số và ứng dụng AI

- *Prompt 1*: Hãy đóng vai một cán bộ chuyển đổi số, xây dựng kế hoạch triển khai chatbot hỗ trợ công dân tra cứu thông tin thuế trực tuyến, bao gồm mục tiêu, công nghệ cần thiết, lộ trình thực hiện, 350 từ, giọng điệu chuyên nghiệp.

- *Prompt 2*: Hãy phân tích dữ liệu công dân bằng AI để xác định các khu vực cần cải thiện dịch vụ y tế công, bao gồm phương pháp phân tích và kết quả dự kiến, 350 từ, giọng điệu phân tích.

- *Prompt 3*: Hãy đề xuất một hệ thống AI để tự động hóa quy trình cấp giấy phép kinh doanh, bao gồm các bước triển khai và lợi ích cho các bộ, công dân, 400 từ, giọng điệu chuyên nghiệp.

Phụ lục II
BẢNG KIỂM TRA NHANH AN TOÀN THÔNG TIN TRƯỚC KHI SỬ DỤNG AI

(Kèm theo Công văn số /SKHCN-BCVTCNTT ngày tháng năm 2026
của Sở Khoa học và Công nghệ)

Stt	Câu hỏi kiểm tra	Có	Không
1	Thông tin tôi sắp nhập có chứa bí mật nhà nước không?	☒	
2	Thông tin tôi sắp nhập có chứa dữ liệu cá nhân (tên, CCCD, SĐT, ...) không?	☒	
3	Thông tin tôi sắp nhập có phải là tài liệu lưu hành nội bộ không?	☒	
4	Tôi có đang dùng email công vụ để đăng ký dịch vụ AI cá nhân hay không?	☒	
5	Mật khẩu tôi đặt cho tài khoản AI này có trùng/tương tự mật khẩu công vụ không?	☒	
6	Tôi có đang tự ý kết nối hệ thống nội bộ của cơ quan vào AI này không?	☒	
7	Nếu câu trả lời là “Có” cho trường hợp 1, 2, 3; tôi có đang sử dụng nền tảng AI nội bộ, được cơ quan cấp phép không?		☒
8	Tôi có biết rõ dữ liệu của mình sẽ được lưu trữ và xử lý ở đâu không?		☒
9	Tôi có kế hoạch kiểm chứng lại kết quả do AI tạo ra không?		☒
10	Nội dung do AI tạo ra có nguy cơ vi phạm tại Điều 7 Luật An ninh mạng (Luật số 116/2025/QH15 ngày 10/12/2025 và có hiệu lực áp dụng từ ngày 01/07/2026) không?	☒	
11	Tôi có sẵn sàng chịu trách nhiệm hoàn toàn về nội dung cuối cùng sau khi đã chỉnh sửa không?		☒
12	Nền tảng AI đang sử dụng có thuộc danh mục được cơ quan, cấp thẩm quyền cho phép hoặc đáp ứng Bộ tiêu chí theo Quyết định số 2847/QĐ-BKHCN ngày 19/6/2026 của Bộ Trưởng Bộ Khoa học và Công nghệ hay không?		☒

Lưu ý: Nếu câu trả lời là CÓ nằm ở ô ☒ thì **TUYỆT ĐỐI DỪNG LẠI** và cân nhắc kỹ lưỡng, tuân thủ các quy định hiện hành.

Phụ lục III
BẢNG THUẬT NGỮ AI THƯỜNG GẶP
(Kèm theo Công văn số /SKHCN- BCVTCNTT ngày tháng năm 2026
của Sở Khoa học và Công nghệ)

- AI (Artificial Intelligence): Trí tuệ nhân tạo
- LLM (Large Language Model): Mô hình ngôn ngữ lớn
- Generative AI: AI tạo sinh, có khả năng tạo ra nội dung mới.
- Hallucination (Ảo giác): Hiện tượng AI đưa ra thông tin sai lệch, bịa đặt.
- Deepfake: Công nghệ tạo ra sản phẩm âm thanh, hình ảnh, video giả một cách chân thực.
- Prompt: Câu lệnh, yêu cầu đầu vào mà người dùng cung cấp cho AI.
- OCR (Optical Character Recognition): Nhận dạng ký tự quang học, công nghệ chuyển đổi hình ảnh chữ viết thành văn bản điện tử.
- Chatbot: Chương trình máy tính mô phỏng cuộc trò chuyện với người dùng.
- Machine Learning (Học máy): là một loại thuật toán AI cho phép máy tính tận dụng nguồn dữ liệu có sẵn để học. Nhờ đó, máy tính được đào tạo để thực hiện những nhiệm vụ như phân loại, dự đoán hoặc khám phá, hỗ trợ ra quyết định và hành động.
- Deep Learning (Học sâu): Tập con chuyên sâu của Học máy, sử dụng các Mạng Nơ-ron Nhân tạo (Neural Networks) nhiều lớp mô phỏng cấu trúc não bộ con người để xử lý các dữ liệu phức tạp như hình ảnh, âm thanh
- NLP (Natural language processing) - Xử lý ngôn ngữ tự nhiên: là khả năng chương trình máy tính hiểu được ngôn ngữ của con người ở nhiều định dạng khác nhau bao gồm ký tự, chữ viết, âm thanh,...

Phụ lục IV

CÁC HÀNH VI VI PHẠM PHỔ BIẾN VÀ VÍ DỤ CẢNH BÁO

(Kèm theo Công văn số /SKHCN-BCVTCNTT ngày tháng năm 2026
của Sở Khoa học và Công nghệ)

Phụ lục này cung cấp các ví dụ cụ thể về hành vi lạm dụng hoặc sử dụng AI sai cách, vi phạm các nguyên tắc bảo mật và an toàn đã nêu trong Hướng dẫn. Cán bộ, đảng viên tuyệt đối không được thực hiện các hành vi này.

1. Nhập dữ liệu nhạy cảm, cá nhân, bí mật lên AI công cộng

- Hành vi sai: Sao chép (copy) nguyên văn một báo cáo nội bộ có đóng dấu "Lưu hành nội bộ" hoặc "Mật" và dán (paste) vào ChatGPT, Claude... với yêu cầu "Tóm tắt báo cáo này".

- Hành vi sai: Tải lên (upload) một file Excel chứa danh sách cán bộ, đảng viên (bao gồm họ tên, ngày sinh, số CCCD, quê quán, chức vụ) lên một công cụ AI phân tích dữ liệu công cộng để "vẽ biểu đồ cơ cấu tổ chức".

- Rủi ro: Lộ lọt vĩnh viễn dữ liệu nội bộ, dữ liệu cá nhân, vi phạm Luật Bảo vệ bí mật nhà nước.

2. Tạo và phát tán nội dung giả mạo (Deepfake)

- Hành vi sai: Sử dụng một công cụ AI tạo sinh video, tải lên hình ảnh của Lãnh đạo A và file ghi âm của Lãnh đạo B để tạo ra một video giả mạo Lãnh đạo A phát biểu nội dung của Lãnh đạo B, dù chỉ với mục đích "thử nghiệm" hoặc "đùa vui" trong nội bộ.

- Rủi ro: Tạo ra thông tin sai lệch nghiêm trọng, gây hoang mang, hiểu lầm, ảnh hưởng trực tiếp đến uy tín của lãnh đạo và tổ chức. Đây là hành vi vi phạm pháp luật nghiêm trọng.

3. Tạo và phát tán nội dung vi phạm pháp luật, thuần phong mỹ tục

- Hành vi sai: Yêu cầu AI "viết một bài phân tích mang tính đả kích" hoặc "bình luận tiêu cực" về một chủ trương, chính sách đang được thảo luận. Sử dụng AI để "viết lại" một tin tức sai sự thật (fake news) sao cho "thuyết phục hơn" để chia sẻ.

- Hành vi sai: Yêu cầu AI tạo ra các hình ảnh, câu chuyện đồi trụy, bạo lực hoặc vi phạm các chuẩn mực đạo đức, văn hóa.

- Rủi ro: Vi phạm Điều 8 Luật An ninh mạng, gây bất ổn xã hội, phá hoại tư tưởng.

4. Vi phạm quy tắc quản lý tài khoản và mật khẩu

- Hành vi sai: Sử dụng email công vụ (ví dụ: nguyenvana@...chinhphu.vn) để đăng ký tài khoản cá nhân trên các nền tảng AI công cộng như ChatGPT,

Gamma...

- Hành vi sai: Đặt mật khẩu cho tài khoản AI cá nhân (ví dụ: tài khoản Claude) trùng với mật khẩu email công vụ hoặc mật khẩu đăng nhập hệ thống nội bộ.

- Rủi ro: Nếu nền tảng AI bị tấn công, kẻ xấu sẽ có được email và mật khẩu công vụ, dẫn đến thâm nhập và đánh cắp toàn bộ dữ liệu trong hệ thống của cơ quan.

5. Lưu mật khẩu tại nơi công cộng

- Hành vi sai: Sử dụng máy tính tại quán cà phê, trung tâm hội nghị hoặc máy tính dùng chung của phòng, đăng nhập vào chatbot AI và chọn "Lưu mật khẩu" (Save Password) trên trình duyệt.

- Rủi ro: Người dùng sau có thể dễ dàng truy cập vào tài khoản, xem lại toàn bộ lịch sử các cuộc hội thoại (prompt) và các thông tin nhạy cảm đã nhập trước đó.

6. Kết nối trái phép hệ thống nội bộ

- Hành vi sai: Một cán bộ có kiến thức về CNTT tự ý viết một đoạn mã (script) để "kết nối" (hook) hệ thống văn bản nội bộ của cơ quan với API của một AI công cộng, nhằm mục đích tự động tóm tắt văn bản đến.

- Rủi ro: Tạo ra một "cửa hậu" (backdoor) không được kiểm soát, vô tình đẩy toàn bộ dữ liệu nội bộ ra bên ngoài mà không qua bất kỳ cơ chế kiểm duyệt, phê duyệt hay bảo vệ nào