

Số: /2026/QĐ-UBND

Hưng Yên, ngày tháng 9 năm 2026

QUYẾT ĐỊNH

**Ban hành Quy chế quản lý, vận hành, khai thác, chia sẻ dữ liệu
và bảo đảm an ninh mạng đối với các hệ thống thông tin,
nền tảng số của tỉnh Hưng Yên (khôi chính quyền)**

ỦY BAN NHÂN DÂN TỈNH HƯNG YÊN

Căn cứ Luật Tổ chức chính quyền địa phương ngày 16 tháng 6 năm 2025;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật ngày 19 tháng 02 năm 2025;

Căn cứ Luật Giao dịch điện tử ngày 22 tháng 6 năm 2023;

Căn cứ Luật Dữ liệu ngày 30 tháng 11 năm 2024;

Căn cứ Luật Bảo vệ dữ liệu cá nhân ngày 26 tháng 6 năm 2025;

Căn cứ Luật An ninh mạng ngày 10 tháng 12 năm 2025;

Căn cứ Luật Bảo vệ bí mật nhà nước ngày 10 tháng 12 năm 2025;

Căn cứ Luật Chuyển đổi số ngày 11 tháng 12 năm 2025;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 165/2025/NĐ-CP ngày 30 tháng 6 năm 2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Dữ liệu;

Căn cứ Nghị định số 194/2025/NĐ-CP ngày 03 tháng 7 năm 2025 của Chính phủ quy định chi tiết một số điều của Luật Giao dịch điện tử về cơ sở dữ liệu quốc gia, kết nối và chia sẻ dữ liệu, dữ liệu mở phục vụ giao dịch điện tử của cơ quan nhà nước;

Căn cứ Nghị định số 278/2025/NĐ-CP ngày 22 tháng 10 năm 2025 của Chính phủ quy định về kết nối, chia sẻ dữ liệu bắt buộc giữa các cơ quan thuộc hệ thống chính trị;

Căn cứ Nghị định số 356/2025/NĐ-CP ngày 31 tháng 12 năm 2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân;

Căn cứ Nghị định số 63/2026/NĐ-CP ngày 28 tháng 02 năm 2026 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ bí mật nhà nước;

Căn cứ Nghị định số 224/2026/NĐ-CP ngày 24 tháng 6 năm 2026 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Chuyển đổi số;

Căn cứ Quyết định số 20/2025/QĐ-TTg của Thủ tướng Chính phủ ban hành Danh mục dữ liệu quan trọng, dữ liệu cốt lõi;

Căn cứ Quyết định số 2439/QĐ-TTg ngày 04 tháng 11 năm 2025 của Thủ tướng Chính phủ ban hành Khung kiến trúc dữ liệu quốc gia, Khung quản trị, quản lý dữ liệu quốc gia, Tờ diễn dữ liệu dùng chung;

Căn cứ Quyết định số 11/2026/QĐ-TTg ngày 28 tháng 3 năm 2026 của Thủ tướng Chính phủ ban hành danh mục cơ sở dữ liệu quốc gia;

Theo đề nghị của Giám đốc Công an tỉnh tại Tờ trình số /TTr-CAT ngày tháng năm 2026.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế quản lý, vận hành, khai thác, chia sẻ dữ liệu và bảo đảm an ninh mạng đối với các hệ thống thông tin, nền tảng số của tỉnh Hưng Yên (khối chính quyền).

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày tháng năm 2026.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh; Giám đốc Công an tỉnh; Giám đốc Sở Khoa học và Công nghệ; Thủ trưởng các sở, ban, ngành tỉnh; Chủ tịch Ủy ban nhân dân các xã, phường và các cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- Như Điều 3;
- Bộ Công an;
- Thường trực Tỉnh ủy; Thường trực HĐND tỉnh;
- Chủ tịch, các Phó Chủ tịch UBND tỉnh;
- Trung tâm Thông tin - Hội nghị tỉnh;
- Lưu: VT.

**TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH**

QUY CHẾ

Quản lý, vận hành, khai thác, chia sẻ dữ liệu và bảo đảm an ninh mạng đối với các hệ thống thông tin, nền tảng số của tỉnh Hưng Yên (khối chính quyền)

*(Ban hành kèm theo Quyết định số /2026/QĐ-UBND ngày tháng 9 năm 2026
của Ủy ban nhân dân tỉnh Hưng Yên)*

Chương I

QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Quy chế này quy định việc quản lý, vận hành, khai thác, kết nối, chia sẻ dữ liệu và bảo đảm an ninh mạng đối với các hệ thống thông tin, nền tảng số, cơ sở dữ liệu và dữ liệu dùng chung của tỉnh Hưng Yên thuộc khối chính quyền; trách nhiệm của các cơ quan, đơn vị, tổ chức, cá nhân có liên quan.

2. Quy chế này áp dụng đối với các sở, ban, ngành tỉnh, Ủy ban nhân dân các xã, phường (sau đây gọi là UBND cấp xã), đơn vị sự nghiệp công lập thuộc tỉnh; cơ quan Trung ương đóng trên địa bàn tỉnh, tổ chức, doanh nghiệp, cá nhân khi tham gia kết nối, chia sẻ, khai thác dữ liệu dùng chung của tỉnh hoặc tham gia xây dựng, vận hành, cung cấp dịch vụ đối với các hệ thống thông tin, nền tảng số của tỉnh.

Cơ quan Đảng, Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội cấp tỉnh khi kết nối, chia sẻ, khai thác dữ liệu dùng chung của tỉnh được áp dụng Quy chế này trên cơ sở thống nhất với cơ quan có thẩm quyền.

3. Quy chế này điều chỉnh đối với dữ liệu không chứa thông tin bí mật nhà nước. Đối với dữ liệu chứa thông tin bí mật nhà nước, dữ liệu quốc phòng, an ninh, cơ yếu và dữ liệu do pháp luật chuyên ngành quy định riêng, việc xác định, quản lý, lưu trữ, khai thác, tiêu hủy thực hiện theo pháp luật tương ứng; riêng các hành vi bị nghiêm cấm tại Điều 4, trách nhiệm rà soát, phân loại trước khi đưa vào danh mục, kết nối, chia sẻ tại khoản 2 Điều 18 và trách nhiệm báo cáo sự cố khẩn cấp tại khoản 2 Điều 19 Quy chế này vẫn được áp dụng đối với dữ liệu chứa thông tin bí mật nhà nước nhằm bảo đảm an ninh chung của hệ thống thông tin, nền tảng số của tỉnh.

4. Trường hợp văn bản quy phạm pháp luật có hiệu lực pháp lý cao hơn hoặc quy chế của bộ, ngành chủ quản cơ sở dữ liệu quy định khác thì áp dụng quy định đó.

Điều 2. Giải thích từ ngữ

Trong Quy chế này, các từ ngữ dưới đây được hiểu như sau:

1. Dữ liệu dùng chung của tỉnh là dữ liệu số do cơ quan nhà nước của tỉnh tạo lập, thu thập, quản lý hoặc tiếp nhận, được đưa vào danh mục dữ liệu dùng chung để chia sẻ, khai thác chung giữa các cơ quan, đơn vị.

2. Dữ liệu gốc là dữ liệu được tạo lập, cập nhật đầu tiên từ nguồn chính thức, dùng làm căn cứ đối chiếu, xác thực, đồng bộ với dữ liệu trùng lặp tại các hệ thống khác.

3. Dữ liệu chủ là dữ liệu chứa thông tin cơ bản, cốt lõi về đối tượng quản lý, dùng làm cơ sở tham chiếu, đồng bộ giữa các cơ sở dữ liệu.

4. Dữ liệu tham chiếu là bảng mã, danh mục dùng chung (mã đơn vị hành chính, mã ngành, lĩnh vực, mã định danh và bảng mã tương tự) được sử dụng thống nhất để phân loại, định danh, liên kết dữ liệu.

5. Đơn vị chủ quản dữ liệu là cơ quan, đơn vị được giao trực tiếp quản lý, cập nhật, chịu trách nhiệm về nội dung, chất lượng dữ liệu và quyết định việc chia sẻ dữ liệu theo thẩm quyền.

6. Đơn vị vận hành kỹ thuật là cơ quan, đơn vị được giao quản lý, vận hành hạ tầng, nền tảng, hệ thống phục vụ lưu trữ, kết nối, chia sẻ dữ liệu dùng chung của tỉnh.

7. Nền tảng tích hợp, chia sẻ dữ liệu của tỉnh (LGSP) là hạ tầng kết nối, chia sẻ dữ liệu cấp tỉnh, kết nối các hệ thống trong tỉnh với nhau và với Nền tảng tích hợp, chia sẻ dữ liệu quốc gia, Nền tảng chia sẻ, điều phối dữ liệu của Trung tâm dữ liệu quốc gia.

8. Kho dữ liệu dùng chung của tỉnh là hệ thống tập hợp, lưu trữ, chuẩn hóa, tổng hợp dữ liệu từ các cơ sở dữ liệu, hệ thống thông tin phục vụ khai thác chung, phân tích, chỉ đạo điều hành.

9. Nền tảng số của tỉnh là hệ thống được xây dựng, triển khai dùng chung nhằm cung cấp chức năng, dịch vụ số phục vụ nhiều cơ quan, đơn vị trên địa bàn tỉnh.

10. Dữ liệu chuyên ngành là dữ liệu hình thành, quản lý theo chức năng quản lý nhà nước của từng ngành, lĩnh vực, phục vụ trực tiếp hoạt động chuyên môn của cơ quan, đơn vị quản lý ngành, lĩnh vực đó.

11. Dữ liệu mở là dữ liệu được cơ quan nhà nước có thẩm quyền công bố công khai theo Điều 7 Quy chế này, cho phép tổ chức, cá nhân tự do khai thác, sử dụng lại và tự chịu trách nhiệm.

12. Dữ liệu chia sẻ có điều kiện là dữ liệu chưa có trong danh mục dữ liệu dùng chung kèm dịch vụ chia sẻ mặc định hoặc dữ liệu được chia sẻ kèm theo điều kiện, giới hạn về phạm vi, mục đích, thời hạn khai thác theo thỏa thuận chia sẻ dữ liệu quy định tại khoản 6 Điều 11 Quy chế này.

13. Dữ liệu cá nhân, dữ liệu cá nhân nhạy cảm được xác định theo quy định của pháp luật về bảo vệ dữ liệu cá nhân.

14. Dữ liệu quan trọng, dữ liệu cốt lõi được xác định theo Danh mục dữ liệu quan trọng, Danh mục dữ liệu cốt lõi do Thủ tướng Chính phủ ban hành và quy định của pháp luật về dữ liệu.

Điều 3. Nguyên tắc quản lý, kết nối, chia sẻ và bảo vệ dữ liệu

1. Dữ liệu hình thành từ hoạt động của cơ quan nhà nước là tài nguyên của tỉnh; mỗi loại dữ liệu có một đơn vị chủ quản; không phân tán, trùng lặp, cát cứ dữ liệu.

2. Mở mặc định, bảo vệ đặc biệt: cơ quan nhà nước có trách nhiệm chia sẻ dữ liệu trong phạm vi quản lý theo chuẩn thống nhất; dữ liệu cá nhân, dữ liệu quan trọng, dữ liệu cốt lõi được bảo vệ theo chế độ tương ứng và chỉ chia sẻ khi đủ điều kiện.

3. Dữ liệu chỉ thu thập một lần, cập nhật tại nguồn, sử dụng nhiều lần; không yêu cầu người dân, doanh nghiệp cung cấp lại thông tin, giấy tờ đã có trong cơ sở dữ liệu.

4. Kết nối, chia sẻ thực hiện thống nhất qua các nền tảng theo Khung kiến trúc dữ liệu quốc gia; ưu tiên chia sẻ thường xuyên, tự động, có phân quyền thay cho đề nghị theo từng vụ việc.

5. Khai thác, sử dụng dữ liệu đúng thẩm quyền, mục đích, phạm vi, thời hạn được phê duyệt.

6. Bảo đảm an ninh, an toàn dữ liệu trong toàn bộ vòng đời dữ liệu; không đánh đổi an ninh, an toàn dữ liệu để lấy tiến độ hoặc sự thuận tiện.

7. Không làm phát sinh thủ tục hành chính, chế độ báo cáo không cần thiết.

Điều 4. Các hành vi bị nghiêm cấm

1. Thu thập, cập nhật, khai thác, chia sẻ, cung cấp, mua bán, công khai dữ liệu trái pháp luật hoặc vượt phạm vi, mục đích, thẩm quyền được giao.

2. Truy cập, chiếm đoạt, làm lộ, làm mất, làm sai lệch, xóa, sửa, phát tán dữ liệu trái phép; sử dụng dữ liệu dùng chung cho mục đích cá nhân, vụ lợi.

3. Cản trở, trì hoãn, từ chối trái quy định việc chia sẻ dữ liệu; cố ý duy trì cát cứ dữ liệu; cung cấp dữ liệu không đầy đủ, không chính xác, không đúng thời hạn.

4. Cung cấp lại dữ liệu cho bên thứ ba khi chưa được cho phép.

5. Dùng chung tài khoản, sử dụng tài khoản của người khác; làm lộ mật khẩu, khóa API, chứng thư số.

6. Che giấu, không báo cáo hoặc báo cáo chậm sự cố dữ liệu.

7. Đưa dữ liệu cá nhân, dữ liệu quan trọng, dữ liệu cốt lõi, dữ liệu chứa thông tin bí mật nhà nước lên hệ thống, nền tảng không đáp ứng yêu cầu bảo vệ.

8. Lợi dụng việc kết nối, chia sẻ, khai thác dữ liệu để theo dõi, giám sát, đánh giá tổ chức, cá nhân trái thẩm quyền.

9. Sử dụng công nghệ trí tuệ nhân tạo (AI), kỹ xảo giả mạo (Deepfake), công cụ tự động hóa hoặc mã độc để thu thập, phân tích, can thiệp trái phép, bóp méo, làm sai lệch hoặc phá hoại dữ liệu của cơ quan nhà nước.

10. Tự ý can thiệp, vô hiệu hóa các giải pháp bảo đảm an ninh mạng, hệ thống giám sát tập trung; thực hiện các hành vi xóa dấu vết, can thiệp làm sai lệch dữ liệu nhật ký hệ thống (log) nhằm cản trở hoạt động giám sát, phát hiện sự cố và điều tra, giám định sự cố.

11. Tạo lập cửa sau (backdoor), mở cổng kết nối từ xa (remote access) không an toàn hoặc cho phép bên thứ ba truy cập trực tiếp vào hệ thống chứa dữ liệu dùng chung mà không qua cơ chế kiểm soát, phân quyền và giám sát an ninh mạng.

Chương II

QUẢN LÝ, VẬN HÀNH HỆ THỐNG THÔNG TIN, NỀN TẢNG SỐ VÀ DỮ LIỆU DÙNG CHUNG

Điều 5. Danh mục dữ liệu của tỉnh

1. Dữ liệu thuộc phạm vi quản lý của tỉnh được rà soát, phân nhóm vào các danh mục: dữ liệu gốc; dữ liệu chủ; dữ liệu tham chiếu; dữ liệu chuyên ngành; dữ liệu dùng chung; dữ liệu mở; dữ liệu chia sẻ có điều kiện.

2. Mỗi dữ liệu trong danh mục phải mô tả tối thiểu: tên, nội dung; đơn vị chủ quản; cấu trúc, định dạng, trường dữ liệu chính; tần suất cập nhật; thời hạn lưu trữ; nhóm chia sẻ; yếu tố dữ liệu cá nhân, dữ liệu quan trọng, dữ liệu cốt lõi (nếu có); phương thức, điều kiện khai thác và biện pháp bảo vệ.

3. Danh mục dữ liệu được chuẩn hóa theo Khung kiến trúc dữ liệu quốc gia, Khung quản trị, quản lý dữ liệu quốc gia và Từ điển dữ liệu dùng chung ban hành kèm theo Quyết định số 2439/QĐ-TTg.

4. Đơn vị chủ quản dữ liệu lập danh mục dữ liệu thuộc phạm vi quản lý gửi Sở Khoa học và Công nghệ. Sở Khoa học và Công nghệ rà soát về chuẩn kỹ thuật, định dạng, mã định danh, tổng hợp, trình Ủy ban nhân dân tỉnh ban hành danh mục dữ liệu dùng chung, danh mục dữ liệu mở; lấy ý kiến Công an tỉnh đối với dữ liệu có yếu tố dữ liệu cá nhân, dữ liệu quan trọng, dữ liệu cốt lõi, an ninh, trật tự. Danh mục được công bố trên Cổng thông tin điện tử tỉnh và rà soát, cập nhật ít nhất mỗi năm một lần.

5. Dữ liệu thuộc cơ sở dữ liệu quốc gia theo Quyết định số 11/2026/QĐ-TTg và dữ liệu thuộc phạm vi kết nối, chia sẻ bắt buộc theo Nghị định số 278/2025/NĐ-CP được ưu tiên chuẩn hóa, kết nối trước.

6. Dữ liệu chứa thông tin bí mật nhà nước không đưa vào danh mục dữ liệu dùng chung, danh mục dữ liệu mở.

Điều 6. Chất lượng dữ liệu

1. Dữ liệu dùng chung phải bảo đảm các tiêu chí:

a) Đúng: chính xác về nghiệp vụ, đúng định dạng, kiểu dữ liệu theo quy định kỹ thuật, được xác thực với dữ liệu gốc;

b) Đủ: đầy đủ trường thông tin bắt buộc; số hóa đầy đủ đối tượng được quản lý;

c) Sạch: đã loại bỏ bản ghi trùng lặp, sai định dạng, lỗi lô-gích, mâu thuẫn, thông tin hết giá trị sử dụng;

d) Sống: cập nhật kịp thời theo thay đổi thực tế; dữ liệu phục vụ thủ tục hành chính, dịch vụ công được đồng bộ ngay khi thay đổi;

đ) Thống nhất: thống nhất về mô hình, cấu trúc, mã định danh, danh mục trên toàn hệ thống;

e) Dùng chung: được tổ chức, kết nối, chia sẻ giữa các cơ quan trên nguyên tắc bảo mật, phân quyền.

2. Chất lượng dữ liệu được kiểm tra ở ba lớp: kiểm tra đầu vào tại đơn vị chủ quản; kiểm tra trong quá trình truyền tải; kiểm tra chéo sau khi đồng bộ tại kho dữ liệu dùng chung.

3. Đơn vị chủ quản dữ liệu tự đánh giá chất lượng dữ liệu thuộc phạm vi quản lý theo các tiêu chí tại khoản 1 Điều này, gửi kết quả về Công an tỉnh để tổng hợp. Kết quả đánh giá được sử dụng trong đánh giá chỉ số chuyên đổi số, thi đua, khen thưởng, xếp loại cơ quan, đơn vị.

Điều 7. Hạ tầng dữ liệu, hệ thống thông tin, nền tảng số của tỉnh

1. Kho dữ liệu dùng chung và nền tảng tích hợp, chia sẻ dữ liệu của tỉnh là hạ tầng dữ liệu tập trung, thống nhất, kết nối với Nền tảng tích hợp, chia sẻ dữ liệu quốc gia và Nền tảng chia sẻ, điều phối dữ liệu của Trung tâm dữ liệu quốc gia. Sở Khoa học và Công nghệ là đơn vị vận hành kỹ thuật, trừ trường hợp Ủy ban nhân dân tỉnh có quyết định khác.

2. Hệ thống thông tin, nền tảng số, cơ sở dữ liệu khi xây dựng mới, nâng cấp phải phù hợp Khung Kiến trúc số của tỉnh, có khả năng kết nối, chia sẻ tự động qua nền tảng tích hợp, chia sẻ dữ liệu của tỉnh; không đầu tư mới hệ thống, cơ sở dữ liệu trùng lặp về chức năng, phạm vi với hệ thống, cơ sở dữ liệu đã có.

3. Mỗi hệ thống thông tin, nền tảng số phải xác định rõ cơ quan chủ quản và đơn vị vận hành kỹ thuật. Đơn vị vận hành kỹ thuật bảo đảm hệ thống hoạt động liên tục, ổn định tối thiểu 99% thời gian; theo dõi, giám sát tình trạng hoạt động; thực hiện bảo trì, cập nhật, xử lý sự cố; lập, lưu giữ hồ sơ quản lý vận hành và hồ sơ cấp độ an toàn hệ thống thông tin.

4. Dữ liệu mở được lựa chọn từ dữ liệu đủ điều kiện công khai, ưu tiên dữ liệu có nhu cầu khai thác cao; công bố kèm điều kiện sử dụng, ở định dạng máy đọc được; không bao gồm dữ liệu cá nhân, dữ liệu hạn chế tiếp cận. Tổ chức, cá nhân được tự do khai thác, sử dụng lại và tự chịu trách nhiệm.

Điều 8. Trách nhiệm của đơn vị chủ quản dữ liệu

1. Chịu trách nhiệm về chất lượng, tính chính xác, tính hợp pháp của dữ liệu thuộc phạm vi quản lý; tổ chức thu thập, cập nhật, chuẩn hóa, làm sạch dữ liệu tại nguồn; đồng bộ lên kho dữ liệu dùng chung ngay khi dữ liệu gốc thay đổi.

2. Lập, cập nhật danh mục dữ liệu; phân loại mức độ chia sẻ, mức độ bảo vệ; quyết định hoặc trình cấp có thẩm quyền quyết định việc chia sẻ dữ liệu; duy trì dịch vụ chia sẻ theo danh mục đã công bố.

3. Kiểm tra, hiệu chỉnh dữ liệu tại nguồn trong thời hạn 05 ngày làm việc kể từ khi nhận phản ánh về dữ liệu sai lệch, thiếu, trùng lặp; trường hợp phức tạp không quá 15 ngày làm việc; thông báo kết quả và đồng bộ dữ liệu đã hiệu chỉnh. Trường hợp sai khác với dữ liệu gốc thì hiệu chỉnh theo dữ liệu gốc. Việc hiệu chỉnh được ghi nhận ký, lưu vết giá trị trước và sau.

4. Cử đầu mối nghiệp vụ, đầu mối kỹ thuật phụ trách công tác dữ liệu.

5. Trường hợp dữ liệu do đơn vị sự nghiệp công lập trực thuộc trực tiếp tạo lập, quản lý thì sở, ngành chủ quản chịu trách nhiệm tổng hợp, lập danh mục dữ liệu và quyết định việc chia sẻ dữ liệu theo thẩm quyền; đơn vị trực thuộc chịu trách nhiệm về chất lượng dữ liệu do mình tạo lập, cập nhật.

Chương III

KẾT NỐI, CHIA SẺ, KHAI THÁC DỮ LIỆU

Điều 9. Mô hình, trình tự và phương thức kết nối, chia sẻ

1. Việc kết nối, chia sẻ dữ liệu thực hiện thống nhất qua hệ thống trung gian theo thứ tự ưu tiên: Nền tảng chia sẻ, điều phối dữ liệu của Trung tâm dữ liệu quốc gia; Nền tảng tích hợp, chia sẻ dữ liệu quốc gia; nền tảng tích hợp, chia sẻ dữ liệu của tỉnh. Kết nối trực tiếp giữa hai hệ thống chỉ thực hiện khi không thể kết nối qua hệ thống trung gian và được cấp có thẩm quyền chấp thuận.

2. Trình tự thiết lập kết nối gồm ba bước: tích hợp hệ thống, thông luồng kết nối, kiểm tra bảo đảm an ninh mạng; kết nối, đồng bộ thử nghiệm theo kịch bản trao đổi dữ liệu và xác nhận kết quả kiểm thử bằng văn bản giữa các bên; vận hành chính thức, định kỳ đánh giá chất lượng, an toàn.

3. Phương thức chia sẻ gồm: chia sẻ mặc định đối với dữ liệu đã có trong danh mục kèm dịch vụ chia sẻ, đơn vị khai thác đăng ký sử dụng và được phê duyệt theo quy trình rút gọn; chia sẻ theo yêu cầu đặc thù đối với dữ liệu chưa có trong danh mục, dữ liệu chia sẻ có điều kiện hoặc khai thác vượt phạm vi đã công bố.

4. Phương thức kỹ thuật gồm dịch vụ chia sẻ qua giao diện lập trình ứng dụng (API), đồng bộ theo bản tin, theo lô hoặc khi có thay đổi, truy cập khai thác trực tuyến; ưu tiên phương thức tự động qua API.

5. Việc kết nối, đồng bộ thực hiện theo từng nhóm cơ sở dữ liệu; ưu tiên cơ sở dữ liệu quốc gia, dữ liệu dùng chung và dữ liệu có tần suất khai thác cao. Chậm nhất đến ngày 31 tháng 12 năm 2026 hoàn thành chuẩn hóa và kết nối, chia sẻ bắt buộc qua Nền tảng chia sẻ, điều phối dữ liệu theo Nghị định số 278/2025/NĐ-CP.

Điều 10. Điều kiện kết nối

Hệ thống thông tin, cơ sở dữ liệu chỉ được kết nối vào nền tảng tích hợp, chia sẻ dữ liệu, kho dữ liệu dùng chung của tỉnh khi đáp ứng đủ các điều kiện:

1. Có hồ sơ đề xuất cấp độ an toàn hệ thống thông tin được phê duyệt và đã triển khai phương án bảo đảm an toàn theo cấp độ; hệ thống kết nối, đồng bộ dữ liệu về Trung tâm dữ liệu quốc gia phải đạt cấp độ 3 trở lên. Trước khi kết nối chính thức vào nền tảng tích hợp, chia sẻ dữ liệu của tỉnh hoặc kho dữ liệu dùng chung, hệ thống phải được kiểm tra, đánh giá an ninh mạng và kiểm thử xâm nhập (penetration testing) thực tế, khắc phục toàn bộ lỗ hổng bảo mật ở mức nghiêm trọng (high, critical) và có văn bản xác nhận an toàn của cơ quan chuyên trách an ninh mạng;

2. Sử dụng mạng truyền số liệu chuyên dùng, kết nối riêng hoặc kênh truyền an toàn tương đương; bảo đảm hoạt động ổn định tối thiểu 99% thời gian, có dự phòng và khả năng mở rộng;

3. Dữ liệu đã được chuẩn hóa, phân loại mức độ chia sẻ và mức độ bảo vệ;

4. Có cơ chế xác thực, phân quyền, ghi nhật ký truy cập theo Điều 17 Quy chế này;

5. Đã hoàn thành kiểm thử theo khoản 2 Điều 9 và được phê duyệt theo Điều 11 Quy chế này.

Điều 11. Quy trình, thẩm quyền phê duyệt và thỏa thuận chia sẻ

1. Đơn vị có nhu cầu khai thác gửi văn bản đề nghị đến đơn vị chủ quản dữ liệu, đồng gửi Sở Khoa học và Công nghệ, nêu rõ: căn cứ, mục đích; loại dữ liệu, phạm vi, trường dữ liệu; phương thức, tần suất, thời hạn khai thác; hệ thống tiếp nhận và cấp độ an toàn hệ thống thông tin; biện pháp bảo vệ dữ liệu; đầu mối chịu trách nhiệm.

2. Trong thời hạn 07 ngày làm việc kể từ ngày nhận đủ hồ sơ, đơn vị chủ quản dữ liệu phê duyệt hoặc trình cấp có thẩm quyền phê duyệt; trường hợp phức tạp, liên quan nhiều cơ quan không quá 15 ngày làm việc. Sau khi được phê duyệt, đơn vị vận hành kỹ thuật phối hợp thiết lập kết nối, cấp quyền, kiểm thử trong thời hạn 10 ngày làm việc.

3. Đơn vị chủ quản dữ liệu phê duyệt việc chia sẻ dữ liệu thuộc phạm vi quản lý. Ủy ban nhân dân tỉnh, Chủ tịch Ủy ban nhân dân tỉnh quyết định đối với: chia sẻ dữ liệu liên ngành; kết nối với cơ sở dữ liệu quốc gia, bộ, ngành, địa phương khác trừ trường hợp pháp luật đã quy định thẩm quyền; chia sẻ dữ liệu cho tổ chức, doanh nghiệp ngoài cơ quan nhà nước; trường hợp có ý kiến khác nhau hoặc vượt thẩm quyền của đơn vị chủ quản dữ liệu.

4. Trước khi phê duyệt việc chia sẻ dữ liệu có chứa dữ liệu cá nhân nhạy cảm, dữ liệu quan trọng, dữ liệu cốt lõi hoặc dữ liệu liên quan an ninh, trật tự, cơ quan phê duyệt lấy ý kiến Công an tỉnh.

5. Việc từ chối chia sẻ chỉ thực hiện khi: pháp luật không cho phép chia sẻ; đề nghị không phù hợp chức năng, nhiệm vụ; hệ thống tiếp nhận không đủ điều

kiện tại Điều 10; dữ liệu không thuộc phạm vi quản lý. Việc từ chối phải trả lời bằng văn bản, nêu rõ lý do và căn cứ pháp lý.

6. Chia sẻ theo yêu cầu đặc thù và chia sẻ dữ liệu có điều kiện phải lập thỏa thuận chia sẻ dữ liệu, gồm: các bên; loại, phạm vi, trường dữ liệu; mục đích; phương thức, tần suất, thời hạn; yêu cầu bảo vệ dữ liệu; trách nhiệm các bên; điều kiện tạm dừng, chấm dứt; xử lý dữ liệu khi kết thúc. Đối với chia sẻ mặc định, điều kiện khai thác công bố kèm dịch vụ chia sẻ thay thế thỏa thuận.

Điều 12. Trách nhiệm các bên; tạm dừng kết nối, thu hồi quyền khai thác

1. Đơn vị cung cấp dữ liệu cung cấp đúng nội dung, phạm vi, phương thức, thời hạn được phê duyệt; bảo đảm chất lượng dữ liệu; duy trì dịch vụ chia sẻ ổn định; thông báo trước ít nhất 05 ngày làm việc khi tạm dừng có kế hoạch.

2. Đơn vị khai thác dữ liệu sử dụng dữ liệu đúng mục đích, phạm vi được phê duyệt; không cung cấp lại cho bên thứ ba khi chưa được phép; bảo vệ dữ liệu tiếp nhận theo Chương IV Quy chế này; chịu trách nhiệm về hậu quả do sử dụng dữ liệu sai quy định.

3. Đơn vị vận hành kỹ thuật bảo đảm hạ tầng kết nối hoạt động liên tục, an toàn, giám sát tập trung; cử đầu mối quản trị dữ liệu, vận hành hệ thống, an ninh thông tin; xây dựng kịch bản xử lý sự cố cho từng dịch vụ chia sẻ; hỗ trợ kỹ thuật và phối hợp xử lý sự cố.

4. Kết nối, quyền khai thác bị tạm dừng khi: có sự cố, nguy cơ mất an toàn dữ liệu, an ninh mạng; hệ thống không còn đáp ứng điều kiện tại Điều 10; bảo trì, nâng cấp có kế hoạch; theo yêu cầu của cơ quan có thẩm quyền.

5. Quyền khai thác bị thu hồi khi: sử dụng dữ liệu sai mục đích, vượt phạm vi; vi phạm quy định về bảo vệ dữ liệu; hết thời hạn khai thác; đơn vị khai thác không còn nhu cầu hoặc không còn chức năng, nhiệm vụ tương ứng.

6. Đơn vị chủ quản dữ liệu quyết định tạm dừng, thu hồi. Đơn vị vận hành kỹ thuật được ngắt kết nối khẩn cấp khi phát hiện sự cố, nguy cơ mất an toàn, đồng thời báo cáo ngay đơn vị chủ quản dữ liệu, Sở Khoa học và Công nghệ, Công an tỉnh. Việc tạm dừng, thu hồi phải thông báo cho các bên liên quan, nêu rõ lý do, thời hạn, điều kiện khôi phục.

Điều 13. Kết nối, chia sẻ dữ liệu với cơ quan Trung ương, địa phương khác và tổ chức, doanh nghiệp

1. Việc kết nối, đồng bộ, chia sẻ dữ liệu với Cơ sở dữ liệu tổng hợp quốc gia, các cơ sở dữ liệu quốc gia, cơ sở dữ liệu của bộ, ngành thực hiện theo pháp luật về dữ liệu, Nghị định số 278/2025/NĐ-CP, Nghị định số 194/2025/NĐ-CP và hướng dẫn, quy chế của cơ quan chủ quản cơ sở dữ liệu. Sở Khoa học và Công nghệ làm đầu mối kỹ thuật; Công an tỉnh phối hợp bảo đảm an ninh, an toàn kết nối.

2. Việc kết nối, chia sẻ, đồng bộ dữ liệu thuộc phạm vi quản lý của lực lượng Công an về Trung tâm dữ liệu quốc gia thực hiện theo Quy chế ban hành

kèm theo Quyết định số 4670/QĐ-BCA-C12 ngày 22 tháng 7 năm 2026 của Bộ trưởng Bộ Công an; Công an tỉnh là đầu mối tổ chức thực hiện.

3. Kết nối, chia sẻ với địa phương khác thực hiện trên cơ sở văn bản thống nhất giữa hai địa phương, qua các nền tảng quy định tại Điều 9 Quy chế này.

4. Chia sẻ dữ liệu cho tổ chức, doanh nghiệp ngoài cơ quan nhà nước chỉ thực hiện khi có căn cứ pháp lý, được Ủy ban nhân dân tỉnh chấp thuận, có thỏa thuận chia sẻ dữ liệu và không bao gồm dữ liệu cá nhân khi chưa đáp ứng điều kiện của pháp luật về bảo vệ dữ liệu cá nhân.

Điều 14. Khai thác, sử dụng dữ liệu

1. Việc khai thác, sử dụng dữ liệu gắn với chức năng, nhiệm vụ của cơ quan, đơn vị, cá nhân được cấp quyền; đúng mục đích, phạm vi, thời hạn được phê duyệt và tuân thủ Chương IV Quy chế này. Kết quả khai thác dữ liệu từ nguồn chính thức có giá trị sử dụng trong hoạt động của cơ quan nhà nước theo pháp luật về giao dịch điện tử.

2. Cơ quan nhà nước và các cơ quan, tổ chức quy định tại khoản 2 Điều 1 Quy chế này khai thác dữ liệu dùng chung của tỉnh không phải trả phí, trừ trường hợp pháp luật có quy định khác.

3. Các cơ quan, đơn vị ưu tiên khai thác dữ liệu từ kho dữ liệu dùng chung, cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành để tự động điền, đối chiếu, xác thực thông tin khi giải quyết thủ tục hành chính; công bố phạm vi thông tin được khai thác thay thế giấy tờ trong thành phần hồ sơ thủ tục hành chính. Dữ liệu phục vụ báo cáo, chỉ đạo điều hành được tổng hợp tự động từ dữ liệu nguồn.

4. Việc sử dụng dữ liệu dùng chung cho hệ thống trí tuệ nhân tạo, mô hình phân tích, dự báo, bảng điều khiển, hệ thống hỗ trợ ra quyết định phải xác định rõ nguồn dữ liệu, phạm vi, trường dữ liệu đưa vào xử lý, huấn luyện, mục đích, biện pháp ẩn danh hóa, mã hóa và cơ chế kiểm tra kết quả đầu ra. Không đưa dữ liệu cá nhân, dữ liệu quan trọng, dữ liệu cốt lõi, dữ liệu chứa thông tin bí mật nhà nước vào hệ thống trí tuệ nhân tạo, nền tảng điện toán đám mây, nền tảng công cộng bên ngoài khi chưa được phê duyệt và chưa đáp ứng điều kiện bảo vệ dữ liệu.

5. Kết quả do hệ thống trí tuệ nhân tạo, công cụ phân tích tự động tạo ra chỉ có giá trị tham khảo, không thay thế trách nhiệm xem xét, quyết định của cơ quan, người có thẩm quyền, trừ trường hợp pháp luật có quy định khác.

Chương IV

BẢO ĐẢM AN NINH MẠNG VÀ AN NINH DỮ LIỆU

Điều 15. Nguyên tắc bảo đảm an ninh mạng, phân loại mức độ bảo vệ dữ liệu và đánh giá rủi ro

1. Bảo đảm an ninh mạng đối với hệ thống thông tin, nền tảng số và bảo đảm an ninh, an toàn dữ liệu là yêu cầu bắt buộc, được thực hiện trong toàn bộ vòng đời dữ liệu, từ tạo lập, thu thập, lưu trữ, truyền nhận, chia sẻ, khai thác đến hủy dữ liệu; bảo đảm tính bí mật, toàn vẹn, sẵn sàng của dữ liệu và khả năng xác thực, truy

vết, trách nhiệm giải trình. Người đứng đầu cơ quan, đơn vị chịu trách nhiệm về công tác này tại cơ quan, đơn vị mình.

2. Dữ liệu được phân loại mức độ bảo vệ gồm: dữ liệu công khai, dữ liệu mở; dữ liệu dùng chung trong cơ quan nhà nước; dữ liệu chia sẻ có điều kiện; dữ liệu cá nhân, dữ liệu cá nhân nhạy cảm; dữ liệu quan trọng; dữ liệu cốt lõi; dữ liệu chứa thông tin bí mật nhà nước. Biện pháp bảo vệ áp dụng tương xứng với mức độ bảo vệ của dữ liệu và cấp độ an toàn của hệ thống.

3. Đơn vị chủ quản dữ liệu đối chiếu dữ liệu thuộc phạm vi quản lý với Danh mục dữ liệu quan trọng, Danh mục dữ liệu cốt lõi ban hành kèm theo Quyết định số 20/2025/QĐ-TTg và danh mục bí mật nhà nước để áp dụng chế độ bảo vệ tương ứng; kết quả phân loại thể hiện trong danh mục dữ liệu. Việc chia sẻ, chuyển giao, xử lý dữ liệu quan trọng, dữ liệu cốt lõi phải được cấp có thẩm quyền phê duyệt sau khi có ý kiến của Công an tỉnh theo trình tự quy định tại khoản 4 Điều 11 Quy chế này.

4. Đơn vị chủ quản dữ liệu, đơn vị vận hành kỹ thuật đánh giá rủi ro an ninh dữ liệu ít nhất một năm một lần và khi có thay đổi lớn về hệ thống, dữ liệu, nhân sự hoặc khi xảy ra sự cố; nội dung gồm nguy cơ, điểm yếu về kỹ thuật, quy trình, nhân sự, mức độ ảnh hưởng và biện pháp giảm thiểu. Kết quả đánh giá là căn cứ điều chỉnh phương án bảo vệ dữ liệu, kế hoạch đầu tư và được tổng hợp trong báo cáo định kỳ. Công an tỉnh hướng dẫn nội dung, phương pháp đánh giá.

Điều 16. An ninh mạng đối với hệ thống, tài khoản, nhân sự và thiết bị

1. Hệ thống thông tin, cơ sở dữ liệu, kho dữ liệu, nền tảng phục vụ dữ liệu dùng chung phải được phê duyệt hồ sơ đề xuất cấp độ và triển khai đầy đủ phương án bảo đảm an toàn theo cấp độ; được kiểm thử bảo mật, đánh giá an toàn trước khi vận hành chính thức và đánh giá định kỳ theo cấp độ được duyệt. Kết quả đánh giá là căn cứ cho phép, duy trì hoặc tạm dừng kết nối.

2. Việc truy cập, khai thác dữ liệu thực hiện qua tài khoản định danh cho từng cá nhân, hệ thống theo nguyên tắc quyền tối thiểu cần thiết; nghiêm cấm dùng chung tài khoản. Tài khoản quản trị, khóa API, chứng thư số được giao đích danh, giám sát sử dụng; áp dụng xác thực nhiều yếu tố đối với tài khoản quản trị và tài khoản truy cập dữ liệu cá nhân nhạy cảm, dữ liệu quan trọng, dữ liệu cốt lõi. Thủ trưởng cơ quan, đơn vị quyết định danh sách người được cấp quyền và rà soát tối thiểu 06 tháng một lần.

3. Người được giao quản trị, vận hành hệ thống, quản lý, khai thác dữ liệu dùng chung phải có cam kết bảo mật bằng văn bản và được tập huấn trước khi cấp quyền. Khi cá nhân chuyển công tác, thôi việc hoặc thay đổi nhiệm vụ, cơ quan, đơn vị thu hồi ngay quyền truy cập, thiết bị được cấp, tổ chức bàn giao tài khoản, khóa truy cập, dữ liệu, tài liệu liên quan và yêu cầu xóa dữ liệu còn lưu trên thiết bị cá nhân. Nghĩa vụ bảo mật tiếp tục được thực hiện sau khi cá nhân không còn đảm nhiệm công việc liên quan.

4. Thiết bị đầu cuối dùng để truy cập, khai thác dữ liệu dùng chung phải được cài đặt, cập nhật phần mềm phòng, chống mã độc, cập nhật bản vá, thiết lập xác thực truy cập và được quản lý, kiểm tra.

5. Việc trích xuất, tải xuống, in ấn, sao chép dữ liệu chỉ thực hiện trong phạm vi được phân quyền và được ghi nhật ký. Dữ liệu đã trích xuất được bảo vệ tương ứng với dữ liệu gốc; không lưu trên thiết bị cá nhân, tài khoản cá nhân, dịch vụ lưu trữ công cộng; được xóa an toàn khi hết mục đích sử dụng.

Điều 17. An ninh mạng trong truyền nhận, lưu trữ; nhật ký, giám sát và sao lưu

1. Dữ liệu truyền nhận giữa các hệ thống phải qua kênh truyền, giao thức an toàn, có xác thực định danh, mã hóa, ký số, kiểm tra toàn vẹn; kết nối qua API phải có xác thực, hạn mức truy vấn, ghi nhật ký, cảnh báo truy cập bất thường. Hạn chế truyền nhận dữ liệu có yêu cầu bảo vệ qua phương thức thủ công, thư điện tử thông thường, thiết bị lưu trữ rời; trường hợp bắt buộc phải mã hóa, lập biên bản giao nhận.

2. Dữ liệu dùng chung của tỉnh được lưu trữ trên hạ tầng đặt tại Việt Nam, đáp ứng cấp độ an toàn tương ứng. Việc lưu trữ, xử lý dữ liệu trên nền tảng, dịch vụ điện toán đám mây hoặc hạ tầng do tổ chức nước ngoài cung cấp, vận hành phải được cấp có thẩm quyền phê duyệt sau khi có ý kiến của Công an tỉnh và Sở Khoa học và Công nghệ. Việc chuyển dữ liệu ra ngoài lãnh thổ Việt Nam thực hiện theo pháp luật về dữ liệu, bảo vệ dữ liệu cá nhân và an ninh mạng.

3. Hệ thống phải ghi nhật ký đầy đủ các thao tác truy cập, khai thác, cập nhật, trích xuất, tải xuống, chia sẻ, phân quyền và thao tác quản trị quan trọng, tối thiểu gồm: tài khoản, thời điểm, địa chỉ hoặc thiết bị truy cập, loại thao tác, phạm vi dữ liệu tác động, kết quả thực hiện và giá trị dữ liệu trước, sau khi thay đổi. Nhật ký được bảo vệ chống sửa, xóa trái phép, lưu giữ tối thiểu 12 tháng; đối với hệ thống dùng chung và dữ liệu cá nhân nhạy cảm, dữ liệu quan trọng, dữ liệu cốt lõi, lưu giữ tối thiểu 24 tháng.

4. Đơn vị vận hành kỹ thuật giám sát liên tục, cảnh báo sớm, phát hiện, ngăn chặn truy cập trái phép, tấn công mạng và truy cập bất thường như đăng nhập bất thường, truy vấn hoặc trích xuất khối lượng lớn, truy cập ngoài phạm vi nhiệm vụ, sử dụng bất thường tài khoản quản trị, can thiệp phân quyền, nhật ký; khi phát hiện, áp dụng ngay biện pháp xác thực bổ sung, khóa phiên, tạm dừng tài khoản hoặc ngắt kết nối và báo cáo theo Điều 19 Quy chế này.

5. Cơ sở dữ liệu, hệ thống dữ liệu dùng chung phải có phương án sao lưu, phục hồi xác định rõ phạm vi, tần suất, vị trí lưu, thời gian lưu và biện pháp bảo vệ bản sao lưu; bản sao lưu được bảo vệ ở mức tương đương hoặc cao hơn dữ liệu gốc. Đơn vị vận hành kỹ thuật thử nghiệm phục hồi tối thiểu mỗi năm một lần.

Điều 18. Bảo vệ dữ liệu cá nhân, dữ liệu bí mật nhà nước và hủy dữ liệu

1. Việc xử lý dữ liệu cá nhân phải có căn cứ pháp lý, đúng mục đích, trong phạm vi tối thiểu cần thiết, có biện pháp phân quyền, ghi nhật ký, mã hóa, ẩn danh hóa phù hợp và bảo đảm quyền của chủ thể dữ liệu. Cơ quan, đơn vị lập, lưu giữ

hồ sơ đánh giá tác động xử lý dữ liệu cá nhân theo pháp luật về bảo vệ dữ liệu cá nhân; đối với dữ liệu cá nhân nhạy cảm phải kiểm soát chặt chẽ người truy cập và lưu vết toàn bộ quá trình khai thác. Công an tỉnh hướng dẫn, kiểm tra việc thực hiện trên địa bàn tỉnh.

2. Dữ liệu chứa thông tin bí mật nhà nước được xác định, quản lý, lưu trữ, truyền nhận, sao chụp, khai thác, tiêu hủy theo pháp luật về bảo vệ bí mật nhà nước và pháp luật về cơ yếu; không lưu trữ, truyền nhận qua hệ thống, thiết bị, dịch vụ không đáp ứng yêu cầu bảo vệ bí mật nhà nước. Đơn vị chủ quản dữ liệu rà soát, phân loại dữ liệu chứa và không chứa thông tin bí mật nhà nước trước khi đưa vào danh mục, kết nối, chia sẻ.

3. Thời hạn lưu trữ của từng loại dữ liệu do đơn vị chủ quản dữ liệu xác định trong danh mục dữ liệu theo pháp luật về lưu trữ và pháp luật chuyên ngành. Dữ liệu hết thời hạn lưu trữ, hết mục đích sử dụng hoặc thuộc trường hợp phải hủy được hủy theo quyết định của người có thẩm quyền; việc hủy phải lập biên bản, ghi nhật ký và bảo đảm dữ liệu không thể khôi phục.

4. Khi thanh lý, điều chuyển, sửa chữa, thay thế thiết bị lưu trữ, máy chủ, thiết bị đầu cuối hoặc chấm dứt sử dụng dịch vụ lưu trữ, cơ quan, đơn vị phải xóa an toàn dữ liệu và lập biên bản xác nhận trước khi bàn giao. Khi kết thúc hợp đồng, đơn vị chủ trì thu hồi đầy đủ dữ liệu, tài khoản, mã nguồn và yêu cầu bên cung cấp dịch vụ xóa toàn bộ dữ liệu của tỉnh còn lưu giữ, có xác nhận bằng văn bản.

Điều 19. Phòng ngừa, xử lý sự cố dữ liệu

1. Sự cố dữ liệu gồm các sự kiện làm lộ, mất, sai lệch, hư hỏng, chiếm đoạt, truy cập trái phép, sử dụng trái phép dữ liệu hoặc gián đoạn dịch vụ kết nối, chia sẻ, khả năng truy cập dữ liệu. Các đơn vị xây dựng kịch bản xử lý sự cố cho từng dịch vụ chia sẻ, đồng bộ dữ liệu và kịch bản xử lý sự cố an ninh mạng.

2. Cơ quan, đơn vị, cá nhân phát hiện sự cố phải thông báo ngay đầu mỗi kỹ thuật, đầu mỗi nghiệp vụ; ngăn chặn, cô lập, ngắt kết nối khi cần thiết; giữ nguyên hiện trạng, không xóa dấu vết, nhật ký; báo cáo đơn vị chủ quản dữ liệu, Sở Khoa học và Công nghệ, Công an tỉnh không quá 24 giờ kể từ khi phát hiện. Đối với sự cố an ninh mạng nghiêm trọng, gồm mã hóa dữ liệu tống tiền (ransomware), tấn công phá hoại, rò rỉ dữ liệu quy mô lớn, lộ lọt bí mật nhà nước, cơ quan, đơn vị phải báo cáo ngay bằng đường dây nóng và gửi văn bản hoặc thông báo kỹ thuật cho Công an tỉnh trong thời hạn không quá 02 giờ kể từ khi phát hiện.

3. Khi phát hiện sự cố tấn công mạng hoặc lộ lọt dữ liệu, đơn vị vận hành kỹ thuật chỉ thực hiện cô lập hệ thống về mặt mạng bằng cách ngắt kết nối Internet, mạng nội bộ; tuyệt đối không tắt nguồn máy chủ, không khởi động lại, không cài đặt lại hệ điều hành, không định dạng ổ đĩa hoặc can thiệp vào bộ nhớ tạm khi chưa có ý kiến và hướng dẫn của lực lượng chuyên trách an ninh mạng thuộc Công an tỉnh, nhằm phục vụ công tác trích xuất chứng cứ, truy tìm dấu vết thủ phạm.

4. Việc xử lý sự cố thực hiện theo trình tự: tiếp nhận, phân loại mức độ; cô lập, ngăn chặn; bảo toàn chứng cứ; xác minh nguyên nhân, phạm vi ảnh hưởng;

khắc phục, phục hồi dữ liệu, hệ thống; thông báo các bên liên quan; đánh giá, hoàn thiện biện pháp phòng ngừa. Dịch vụ kết nối, chia sẻ, đồng bộ dữ liệu phải được khôi phục trong thời hạn tối đa 01 ngày làm việc; quá thời hạn này, đơn vị vận hành kỹ thuật báo cáo Ủy ban nhân dân tỉnh phương án xử lý.

5. Sở Khoa học và Công nghệ điều phối xử lý sự cố kỹ thuật trên hệ thống dùng chung; Công an tỉnh chủ trì xử lý sự cố an ninh mạng, sự cố có dấu hiệu tội phạm, lộ lọt dữ liệu cá nhân, dữ liệu quan trọng, dữ liệu cốt lõi, bí mật nhà nước.

6. Đối với sự cố vi phạm quy định về bảo vệ dữ liệu cá nhân, cơ quan, đơn vị thông báo cho cơ quan chuyên trách bảo vệ dữ liệu cá nhân chậm nhất 72 giờ kể từ thời điểm phát hiện. Sau khi xử lý, cơ quan, đơn vị đề xảy ra sự cố khắc phục hậu quả, phục hồi dữ liệu bị ảnh hưởng, thông báo cho tổ chức, cá nhân bị ảnh hưởng và báo cáo kết quả.

Điều 20. An ninh dữ liệu trong đầu tư, thuê dịch vụ và trách nhiệm của nhà thầu

1. Dự án, hoạt động mua sắm, thuê dịch vụ công nghệ thông tin có xây dựng, nâng cấp cơ sở dữ liệu, kho dữ liệu, nền tảng chia sẻ dữ liệu hoặc có xử lý dữ liệu cá nhân nhạy cảm, dữ liệu quan trọng, dữ liệu cốt lõi phải lấy ý kiến Sở Khoa học và Công nghệ về kiến trúc, chuẩn kỹ thuật và ý kiến Công an tỉnh về an ninh mạng, an ninh dữ liệu trước khi phê duyệt.

2. Nhà thầu, tổ chức, doanh nghiệp tham gia xây dựng, vận hành, bảo trì, nâng cấp, xử lý, lưu trữ hệ thống, dữ liệu của tỉnh phải ký cam kết bảo mật; chỉ tiếp cận hệ thống, dữ liệu, mã nguồn, tài khoản trong phạm vi được giao; không sao chép, lưu giữ, chuyển giao, thương mại hóa dữ liệu; không sử dụng dữ liệu của tỉnh để huấn luyện, kiểm thử, phát triển sản phẩm, dịch vụ, mô hình trí tuệ nhân tạo ngoài phạm vi hợp đồng; không chuyển giao công việc liên quan đến dữ liệu cho bên thứ ba khi chưa được cho phép. Nghiêm cấm nhà thầu sử dụng môi trường thật chứa dữ liệu công dân, dữ liệu quản lý nhà nước để phục vụ mục đích lập trình, kiểm thử tính năng; việc lập trình, kiểm thử phải thực hiện trên môi trường riêng với dữ liệu giả lập hoặc dữ liệu đã được ẩn danh hóa.

3. Hợp đồng phải có điều khoản về bảo vệ dữ liệu, an ninh mạng, quản lý nhân sự và quyền truy cập, thông báo sự cố, quyền kiểm tra của cơ quan nhà nước, bàn giao và xóa dữ liệu khi kết thúc hợp đồng theo khoản 4 Điều 18 Quy chế này và trách nhiệm bồi thường thiệt hại. Nhà thầu vi phạm bị xử lý theo hợp đồng, theo pháp luật và bị xem xét hạn chế, chấm dứt tham gia cung cấp dịch vụ cho các hệ thống dữ liệu của tỉnh.

Chương V

TỔ CHỨC THỰC HIỆN

Điều 21. Sở Khoa học và Công nghệ

1. Chủ trì tham mưu Ủy ban nhân dân tỉnh quản lý nhà nước về hệ thống thông tin, nền tảng số và hạ tầng kỹ thuật của tỉnh; xây dựng, vận hành, nâng cấp kho dữ liệu dùng chung, nền tảng tích hợp, chia sẻ dữ liệu; phối hợp với các cơ

quan, đơn vị khi xây dựng các nền tảng số dùng chung của tỉnh do cơ quan, đơn vị khác chủ trì; làm đầu mối kỹ thuật kết nối với các nền tảng, cơ sở dữ liệu của Trung ương.

2. Rà soát về chuẩn kỹ thuật, tổng hợp, trình ban hành và công bố danh mục dữ liệu của tỉnh; hướng dẫn quy trình kỹ thuật, tiêu chuẩn kết nối theo quy định của bộ, ngành Trung ương.

3. Theo dõi tình trạng hoạt động của các hệ thống thông tin, nền tảng số dùng chung; điều phối xử lý sự cố kỹ thuật; phối hợp với Công an tỉnh trong kiểm tra việc thực hiện Quy chế và xử lý sự cố an ninh mạng.

Điều 22. Công an tỉnh

1. Chủ trì tham mưu, hướng dẫn, kiểm tra việc thực hiện Chương IV Quy chế này và các quy định về an ninh mạng đối với hệ thống thông tin, nền tảng số của tỉnh, an ninh dữ liệu, bảo vệ dữ liệu cá nhân, dữ liệu quan trọng, dữ liệu cốt lõi, bảo vệ bí mật nhà nước; hướng dẫn nội dung, phương pháp đánh giá rủi ro an ninh dữ liệu; giám sát an ninh mạng và cảnh báo kịp thời cho các cơ quan, đơn vị.

2. Cho ý kiến trước khi cấp có thẩm quyền phê duyệt: việc chia sẻ dữ liệu quy định tại khoản 4 Điều 11 và khoản 3 Điều 15; việc lưu trữ, xử lý dữ liệu trên hạ tầng, dịch vụ của tổ chức nước ngoài; các dự án, hoạt động mua sắm, thuê dịch vụ quy định tại khoản 1 Điều 20 Quy chế này.

3. Chủ trì xử lý sự cố an ninh mạng; xác minh, xử lý các vụ việc lộ lọt, chiếm đoạt, tấn công mạng, sử dụng trái phép dữ liệu theo thẩm quyền.

4. Là đầu mối tổ chức kết nối, chia sẻ, đồng bộ dữ liệu thuộc phạm vi quản lý của lực lượng Công an về Trung tâm dữ liệu quốc gia; phối hợp Sở Khoa học và Công nghệ trong kết nối các hệ thống của tỉnh với Trung tâm dữ liệu quốc gia và các cơ sở dữ liệu do Bộ Công an quản lý; tổ chức tập huấn, diễn tập về an ninh dữ liệu.

5. Chủ trì, phối hợp với các cơ quan liên quan tổ chức thanh tra, kiểm tra định kỳ hoặc đột xuất công tác bảo đảm an ninh mạng, bảo vệ dữ liệu cá nhân và bảo vệ bí mật nhà nước đối với các hệ thống thông tin, nền tảng số của tỉnh; có quyền yêu cầu tạm dừng kết nối, ngắt kết nối hoặc đình chỉ vận hành đối với hệ thống vi phạm nghiêm trọng quy chuẩn kỹ thuật về an ninh mạng, có nguy cơ gây hậu quả đặc biệt nghiêm trọng đến an ninh quốc gia, trật tự an toàn xã hội.

6. Hướng dẫn biện pháp bảo đảm an ninh mạng trên các hệ thống thông tin, nền tảng số dùng chung của tỉnh; vận hành hệ thống giám sát an ninh mạng; ban hành biểu mẫu, hướng dẫn thống nhất phục vụ thực hiện Quy chế; kiểm tra việc thực hiện Quy chế về quản lý danh mục dữ liệu, quản lý vận hành hệ thống, kết nối, chia sẻ và chất lượng dữ liệu.

7. Theo dõi, đôn đốc, tổng hợp tình hình thực hiện Quy chế; tổng hợp kết quả tự đánh giá chất lượng dữ liệu của các cơ quan, đơn vị; định kỳ báo cáo Ủy ban nhân dân tỉnh và Bộ Công an theo quy định.

Điều 23. Các sở, ban, ngành, UBND cấp xã và cá nhân được cấp quyền

1. Các sở, ban, ngành, UBND cấp xã thực hiện trách nhiệm của đơn vị chủ quản dữ liệu, đơn vị khai thác dữ liệu theo Quy chế này; phân công đầu mối phụ trách công tác dữ liệu; rà soát hiện trạng hệ thống thông tin, cơ sở dữ liệu; lập, cập nhật danh mục dữ liệu; thực hiện kết nối, chia sẻ theo danh mục và lộ trình được phê duyệt; tổ chức thực hiện các biện pháp bảo đảm an ninh, an toàn dữ liệu quy định tại Chương IV Quy chế này.

2. UBND cấp xã tổ chức thu thập, cập nhật dữ liệu phát sinh tại địa bàn; khai thác dữ liệu phục vụ giải quyết thủ tục hành chính, quản lý địa bàn; kịp thời phản ánh dữ liệu sai lệch và khó khăn, vướng mắc.

3. Văn phòng Ủy ban nhân dân tỉnh theo dõi việc khai thác dữ liệu phục vụ chỉ đạo điều hành và kết nối dữ liệu phục vụ giải quyết thủ tục hành chính trên Hệ thống thông tin giải quyết thủ tục hành chính của tỉnh. Sở Tư pháp phối hợp rà soát tính pháp lý khi được đề nghị. Sở Tài chính tham mưu bố trí kinh phí thực hiện Quy chế.

4. Cán bộ, công chức, viên chức, người lao động được cấp quyền khai thác dữ liệu đúng phạm vi được phân quyền; bảo mật tài khoản, phương thức xác thực; kịp thời báo cáo khi phát hiện dữ liệu sai lệch, truy cập bất thường, sự cố dữ liệu; chịu trách nhiệm trước pháp luật và trước thủ trưởng cơ quan, đơn vị về hoạt động khai thác dữ liệu bằng tài khoản được cấp.

Điều 24. Chế độ báo cáo, kiểm tra và xử lý vi phạm

1. Các cơ quan, đơn vị báo cáo định kỳ hằng năm trước ngày 15 tháng 12 về công tác quản lý, kết nối, chia sẻ, khai thác dữ liệu, kết quả bảo đảm an ninh, an toàn dữ liệu và đánh giá rủi ro bằng một báo cáo hợp nhất theo biểu mẫu do Công an tỉnh ban hành, gửi Công an tỉnh; nội dung về hạ tầng kỹ thuật, vận hành hệ thống thông tin, nền tảng số đồng gửi Sở Khoa học và Công nghệ. Báo cáo đột xuất thực hiện khi xảy ra sự cố hoặc theo yêu cầu của cơ quan có thẩm quyền. Ưu tiên tổng hợp báo cáo tự động từ dữ liệu hệ thống.

2. Hoạt động kết nối, chia sẻ, khai thác, bảo vệ dữ liệu được giám sát thường xuyên bằng công cụ kỹ thuật và kiểm tra định kỳ, đột xuất. Kết luận kiểm tra được gửi đối tượng kiểm tra; đối tượng kiểm tra có trách nhiệm khắc phục tồn tại đúng thời hạn.

3. Cơ quan, đơn vị, cá nhân không thực hiện, thực hiện không đúng, không đầy đủ Quy chế này, tùy tính chất, mức độ, bị xử lý kỷ luật, xử phạt vi phạm hành chính hoặc truy cứu trách nhiệm hình sự; gây thiệt hại phải bồi thường theo quy định của pháp luật. Kết quả thực hiện Quy chế, kết quả đánh giá chất lượng dữ liệu và xử lý vi phạm được xem xét trong đánh giá xếp loại mức độ hoàn thành nhiệm vụ, chỉ số chuyển đổi số, thi đua, khen thưởng hằng năm.

4. Hồ sơ kiểm tra, đánh giá rủi ro, sự cố và xử lý vi phạm được lập, quản lý, lưu trữ theo quy định về công tác văn thư, lưu trữ, bảo đảm phục vụ truy vết, xác minh trách nhiệm.

Điều 25. Lộ trình, kinh phí và điều khoản chuyển tiếp

1. Trong thời hạn 30 ngày kể từ ngày Quy chế có hiệu lực, các cơ quan, đơn vị phân công đầu mối công tác dữ liệu; Công an tỉnh ban hành biểu mẫu, hướng dẫn thống nhất. Trong thời hạn 90 ngày, các cơ quan, đơn vị hoàn thành rà soát hiện trạng, lập danh mục dữ liệu và đánh giá rủi ro an ninh dữ liệu lần đầu. Trong thời hạn 150 ngày, Sở Khoa học và Công nghệ trình Ủy ban nhân dân tỉnh ban hành danh mục dữ liệu dùng chung, danh mục dữ liệu mở phiên bản đầu tiên.

2. Ủy ban nhân dân tỉnh ban hành Kế hoạch triển khai chi tiết, xác định nhóm dữ liệu ưu tiên, nhiệm vụ, cơ quan chủ trì, thời hạn và nguồn lực thực hiện, bảo đảm hoàn thành kết nối, chia sẻ bắt buộc trước ngày 31 tháng 12 năm 2026.

3. Kinh phí thực hiện Quy chế được bảo đảm từ ngân sách nhà nước theo phân cấp, nguồn kinh phí chuyển đổi số và các nguồn hợp pháp khác; ưu tiên bố trí cho nhiệm vụ bảo đảm an ninh, an toàn dữ liệu.

4. Hệ thống thông tin, cơ sở dữ liệu, kết nối, thỏa thuận chia sẻ đã thiết lập trước ngày Quy chế có hiệu lực được tiếp tục sử dụng; trong thời hạn 12 tháng, các cơ quan, đơn vị hoàn thành rà soát, điều chỉnh cho phù hợp với Quy chế này; trường hợp không thể điều chỉnh thì chấm dứt.

5. Đối với hệ thống thông tin, cơ sở dữ liệu, kho dữ liệu hình thành từ tỉnh Hưng Yên và tỉnh Thái Bình trước khi hợp nhất, Sở Khoa học và Công nghệ chủ trì tham mưu phương án hợp nhất hoặc lựa chọn hệ thống sử dụng chính thức, chuyển đổi, đồng bộ dữ liệu lịch sử, chuẩn hóa mã định danh đơn vị hành chính sau sắp xếp, xử lý an toàn dữ liệu trên các hệ thống không tiếp tục sử dụng; hoàn thành theo lộ trình do Ủy ban nhân dân tỉnh quyết định.

6. Thủ trưởng các sở, ban, ngành, Chủ tịch UBND cấp xã và các cơ quan, tổ chức, cá nhân liên quan có trách nhiệm tổ chức thực hiện Quy chế này. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, các cơ quan, đơn vị phản ánh về Sở Khoa học và Công nghệ để tổng hợp, báo cáo Ủy ban nhân dân tỉnh xem xét sửa đổi, bổ sung./.