ỦY BAN NHÂN DÂN TỈNH QUẢNG NAM	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1218/QĐ-UBND	*Quảng Nam, ngày 14 tháng 6 năm 2023*

QUYẾT ĐỊNH

Ban hành Quy định đảm bảo an ninh an toàn hệ thống và dữ liệu; bảo vệ dữ liệu cá nhân trong quá trình kết nối chia sẻ dữ liệu dân cư trong thực hiện Đề án Phát triển ứng dụng dữ liệu dân cư, định danh và xác thực điện tử phục vụ chuyển đổi số quốc gia giai đoạn 2022-2025, tầm nhìn đến năm 2030 của Chính phủ (Đề án 06) trên địa bàn tỉnh Quảng Nam

ỦY BAN NHÂN DÂN TỈNH QUẢNG NAM

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19/6/2015; Luật sửa đổi, bổ sung một số điều của Luật Tổ chức chính phủ số 76/2015/QH13 và Luật Tổ chức chính quyền địa phương số 77/2015/QH13 ngày 22/11/2019;

Căn cứ Nghị định số 26/2020/NĐ-CP, ngày 28/02/2020 của Chính phủ quy định chi tiết một số điều của Luật Bảo vệ bí mật nhà nước;Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về Bảo vệ dữ liệu cá nhân;

Căn cứ Quyết định số 06/QĐ-TTg, ngày 06/01/2022 của Thủ tướng Chính phủ về phê duyệt Đề án Phát triển ứng dụng dữ liệu dân cư, định danh và xác thực điện tử phục vụ chuyển đổi số quốc gia giai đoạn 2022-2025, tầm nhìn đến năm 2030 của Chính phủ;

Căn cứ Thông tư số 46/2022/TT-BCA ngày 04/11/2022 của Bộ Công an quy định về kết nối, chia sẻ và khai thác thông tin giữa Cơ sở dữ liệu quốc gia về dân cư với cơ sở dữ liệu quốc gia, cơ sở dữ liệu chuyên ngành và hệ thống thông tin khác.

Căn cứ Kế hoạch số 1543/KH-UBND ngày 16/3/2022 của Ủy ban nhân dân tỉnh về Triển khai thực hiện Đề án phát triển ứng dụng dữ liệu dân cư, định danh và xác thực điện tử phục vụ chuyển đổi số quốc gia giai đoạn 2022- 2025, tầm nhìn đến năm 2030;

Theo đề nghị của Công an tỉnh tại Tờ trình số 2322 /TTr-CAT-PA06 ngày 02 tháng 06 năm 2023.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy định đảm bảo an ninh an toàn hệ thống và dữ liệu; bảo vệ dữ liệu cá nhân trong quá trình kết nối chia sẻ dữ liệu dân cư trong việc triển khai thực hiện Đề án Phát triển ứng dụng dữ liệu dân cư, định danh và xác thực điện tử phục vụ chuyển đổi số quốc gia giai đoạn 2022-2025, tầm nhìn đến năm 2030 của Chính phủ trên địa bàn tỉnh Quảng Nam.

Điều 2. Quyết định này có hiệu lực thi hành từ ngày ký ban hành.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh; Giám đốc Công an tỉnh; Thủ trưởng các Sở, Ban, ngành trực thuộc UBND tỉnh, Chủ tịch Ủy ban nhân dân các huyện, thị xã, thành phố và các cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- TT Tỉnh ủy; TT HĐND tỉnh;
- Chủ tịch, các PCT UBND tỉnh;
- Đài PT-TH tỉnh, Báo Quảng Nam;
- Cổng TTĐT tỉnh;
- Bưu điện tỉnh, VNPT Quảng Nam;
- PCVP;
- Lưu: VT, NCKS (Thảo).

C:\Users\Admin\OneDrive\Nam 2023\CĐ_ĐH\QĐ quy che ATAN he thong, du lieu ca nhan.docx

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Hồ Quang Bửu

ỦY BAN NHÂN DÂN TỈNH QUẢNG NAM	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY ĐỊNH
Đảm bảo an ninh an toàn hệ thống và dữ liệu; bảo vệ dữ liệu cá nhân trong quá trình kết nối chia sẻ dữ liệu dân cư trong thực hiện Đề án Phát triển ứng dụng dữ liệu dân cư, định danh và xác thực điện tử phục vụ chuyển đổi số quốc gia giai đoạn 2022-2025, tầm nhìn đến năm 2030 của Chính phủ trên địa bàn tỉnh Quảng Nam

(Ban hành kèm theo Quyết định số 1218/QĐ-UBND ngày 14tháng 6 năm 2023 của UBND tỉnh Quảng Nam)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy định này quy định về hoạt động đảm bảo an ninh, an toàn thông tin hệ thống thiết bị, phương tiện, tiêu chuẩn kỹ thuật quản lý, sử dụng, chế tài xử lý, trách nhiệm của các tổ chức cá nhân trong thực hiện Đề án 06 trên địa bàn tỉnh Quảng Nam.

Điều 2. Đối tượng áp dụng

Quy định này áp dụng đối với các cơ quan, Ban, ngành, đoàn thể, địa phương *(gọi tắt là cơ quan, đơn vị, địa phương)* và các tổ chức, cá nhân có liên quan trong thực hiện Đề án 06 trên địa bàn tỉnh Quảng Nam.

Điều 3. Giải thích từ ngữ

1. Đề án 06 là đề án về ứng dụng Cơ sở dữ liệu quốc gia về dân cư, hệ thống định danh và xác thực điện tử, thẻ căn cước công dân gắn chíp điện tử trong công cuộc chuyển đổi số quốc gia một cách linh hoạt, sáng tạo để phục vụ 05 nhóm lợi ích, cụ thể: phục vụ giải quyết thủ tục hành chính và cung cấp dịch vụ công trực tuyến; phục vụ phát triển kinh tế xã hội; phục vụ công dân số, hoàn thiện hệ sinh thái; phục vụ kết nối, khai thác bổ sung làm giàu dữ liệu dân cư; phục vụ chỉ đạo điều hành của lãnh đạo các cấp.

2. Kết nối hệ thống được hiểu là các thiết bị phần mềm kết nối trực tiếp vào Hệ thống Cơ sở dữ liệu quốc gia về dân cư qua mạng chuyên dụng của Bộ Công an theo quy định hoặc kết nối trực tiếp vào hạ tầng, nền tảng tích hợp chia sẻ dữ liệu của tỉnh để khai thác Cơ sở dữ liệu quốc gia về dân cư theo hướng dẫn của Bộ Công an, Bộ Thông tin và Truyền thông và Văn phòng Chính phủ.

3. Người được phép nắm giữ thông tin bảo mật là những người có tên được đăng ký tham gia trực tiếp vào Hệ thống thông tin giải quyết thủ tục hành chính; Thủ trưởngcơ quan, đơn vị kết nối vào hệ thống; lãnh đạo, cán bộ thực hiện công tác quản trị hệ thống thuộc Đề án 06.

4. Đảm bảo an ninh, an toàn thông tin hệ thống là các phương tiện, thiết bị, phần mềm phục vụ cho việc kết nối vào hệ thống dữ liệu thuộc Đề án 06 phải được kiểm tra đánh giá an ninh, an toàn thông tin đảm bảo theo các quy định của pháp luật về bảo vệ bí mật nhà nước.

5. Phòng chống thu thập bí mật nhà nước qua hệ thống các phương tiện, thiết bị, phần mềm là hoạt động ngăn chặn không cho các đối tượng sử dụng các thiết bị, phương tiện, phần mềm tấn công vào hệ thống nhằm thu thập thông tin, tài liệu của hệ thống.

6. Nội dung thực hiện an toàn thông tin là sự bảo vệ thông tin số và các hệ thống thông tin tránh bị truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trực tiếp nhằm đảm bảo tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

7. Nội dung an ninh thông tin là đảm bảo thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức cá nhân.

8. Nội dung bảo mật thông tin là việc đảm bảo bí mật về thông tin trong hệ thống.

9. Thông tin bảo mật là tất cả các thông tin trên hệ thống, cơ quan, đơn vị khai thác, xác thực thông tin không được cung cấp cho bên thứ ba hoặc sử dụng thông tin bảo mật vì bất kỳ lý do gì.

10. Dữ liệu cá nhân là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự trên môi trường điện tử gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể. Dữ liệu cá nhân bao gồm dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm.

11. Bảo vệ dữ liệu cá nhân trong quá trình kết nối chia sẻ dữ liệu dân cư giữa hệ thống thông tin giải quyết thủ tục hành chính trên địa bàn tỉnh Quảng Nam với Cơ sở dữ liệu quốc gia về dân cư và các hệ thống thông tin khác là việc phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm quy định của pháp luật về dữ liệu cá nhân.

Chương II
QUY ĐỊNH VỀ TIÊU CHUẨN KỸ THUẬT VÀ QUẢN LÝ SỬ DỤNG THIẾT BỊ, PHƯƠNG TIỆN PHẦN MỀM THEO ĐỀ ÁN 06

Điều 4. Tiêu chuẩn kỹ thuật cần đáp ứng đối với thiết bị

STT	TÊN THIẾT BỊ	CẤU HÌNH THIẾT BỊ VÀ PHẦN MỀM ỨNG DỤNG
1	Máy tính	- Cấu hình thông số kỹ thuật, phần mềm tối thiểu: + Bộ vi xử lý Intel Core i5 thế hệ 10 tốc độ 1.6Ghz trở lên; Bộ nhớ 8Gb DDR4; Ổ cứng SSD 512Gb; Màn hình tối thiểu 18,5 inch đối với máy tính để bàn; 14 inch đối với máy tính xách tay; + Hệ điều hành: Window10 Pro 64 bit bản quyền, Mac OS, Linux và các phiên bản khác đảm bảo phiên bản mới nhất và thiết lập các chính sách tường lửa bảo vệ máy tính phù hợp; + Phần mềm ứng dụng, bảo vệ hệ thống: BKAV Endpoint kích hoạt bản quyền; Unikey, TayNguyen Key; các phần mềm chuyên dùng khác theo quy định của ngành công an được phép cài đặt, vận hành trên máy vi tính. - Tất cả các phần mềm đều được cài đặt phiên bản mới nhất theo từng thời điểm, loại bỏ, vô hiệu hóa tính năng thu, phát Wifi.
2	Các thiết bị ngoại vi khác kết nối vào hệ thống	Kiểm tra an ninh, an toàn thông tin tiêu chuẩn kỹ thuật trước khi kết nối vào hệ thống.

Điều 5. Quy định về quản lý, sử dụng thiết bị, phần mềm đảm bảo an ninh, an toàn thông tin

1. Phạm vi áp dụng

1.1. Các thiết bị, phương tiện, phần mềm được trang cấp cho các cơ quan, đơn vị, địa phương thực hiện Đề án 06.

1.2. Các thiết bị được các cơ quan, đơn vị, địa phương thực hiện Đề án 06 tự trang bị bổ sung hoặc thay thế để kết nối với hệ thống.

2. Vị trí và các điều kiện đảm bảo khi lắp đặt thiết bị

2.1. Thiết bị phải được đặt ở vị trí nơi làm việc của cơ quan, đơn vị đảm bảo điều kiện về hạ tầng (diện tích, nhiệt độ, độ ẩm...) đảm bảo hoạt động lâu dài của thiết bị, tránh tình trạng không đảm bảo nhiệt độ, độ ẩm, gây hư hỏng các bộ phận phần cứng.

2.2. Không được tự ý di chuyển thiết bị ra khỏi nơi bảo quản khi chưa có sự đồng ý của lãnh đạo cơ quan, đơn vị.

2.3. Thường xuyên vệ sinh sạch sẽ thiết bị và nơi đặt thiết bị.

3. Các hành vi bị nghiêm cấm trong quá trình sử dụng các thiết bị kết nối vào hệ thống của Đề án 06

3.1. Các hành vi bị nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng.

3.2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập mạng không dây của cá nhân vào mạng hệ thống Đề án 06 khi chưa được sự đồng ý, hướng dẫn của Công an tỉnh Quảng Nam, trên cùng một thiết bị thực hiện đồng thời truy cập vào mạng nội bộ và truy cập internet bằng thiết bị kết nối internet của cá nhân (USB 3G/4G, điện thoại di động, máy tính bảng, máy tính xách tay...)

3.3. Tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin (gỡ bỏ phần mềm diệt virus, tắt Window Defender trên hệ điều hành Windows và các phần mềm bảo vệ khác đã được cài đặt) tự ý thay thế, lắp mới, trao đổi thành phần của máy tính phục vụ vào mục đích khác mà không có sự đồng ý hướng dẫn *"làm sạch"* của Công an tỉnh Quảng Nam.

3.4. Tạo ra, cài đặt, phát tán phần mềm độc hại gây ảnh hưởng đến hoạt động bình thường của hệ thống thông tin. Tự ý cài đặt phần mềm không thuộc danh sách các phần mềm được sử dụng tại Điều 4 của Quy định này.

3.5 Thu thập, sử dụng, tán phát trái phép thông tin cá nhân nằm trong hệ thống, lợi dụng sơ hở, thiếu sót của hệ thống để thu thập, khai thác thông tin công dân.

4. Quản lý sử dụng thiết bị

4.1. Thực hiện theo Luật Bảo vệ bí mật nhà nước ngày 15/11/2018, Nghị định số 26/2020/NĐ-CP ngày 28/02/2020 của Chính phủ; Quyết định số 30/2021/QĐ-UBND của UBND tỉnh Quảng Nam Ban hành Quy chế bảo vệ bí mật nhà nước trên địa bàn tỉnh Quảng Nam.

4.2. Đối với máy tính phục vụ khai thác cập nhật hệ thống Đề án 06 thì quản lý, sử dụng như sau: Ổ đĩa cứng máy tính được quản lý sử dụng như một thiết bị lưu trữ dữ liệu có tính bảo mật cao. Khi bảo hành sửa chữa, không được tự ý mang ổ đĩa cứng ra khỏi cơ quan, đơn vị. Khi ổ đĩa cứng hỏng hoặc chuyển

đổi mục đích sử dụng, mang đi bảo hành phải trao đổi Công an tỉnh để được hướng dẫn thực hiện theo quy định.

4.3. Lãnh đạo cơ quan, đơn vị phải bố trí cán bộ và gắn trách nhiệm trực tiếp cho việc quản lý sử dụng thiết bị đảm bảo an ninh an toàn theo quy định, định kỳ cập nhật phần mềm.

4.4. Máy tính và các thiết bị ngoại vi trước khi kết nối vào hệ thống phải được Công an tỉnh kiểm tra an ninh, an toàn thông tin.

4.5. Quá trình sử dụng, cán bộ quản lý không được tự ý thay đổi các tham số cài đặt trên thiết bị *(địa chỉ IP, quy tắc an ninh, an toàn thông tin...)*. Trường hợp cần thiết phải thay đổi, cán bộ có trách nhiệm báo cáo cơ quan, đơn vị, có văn bản trao đổi thông báo Công an tỉnh để xử lý (*trường hợp tự ý thay đổi khi không được sự đồng ý của các đơn vị chức năng sẽ bị xử lý trách nhiệm theo quy định*).

4.6. Khi phát hiện các thiết bị gặp sự cố hỏng hóc, có dấu hiệu, nguy cơ mất an ninh, an toàn thông tin, cán bộ quản lý báo cáo cơ quan, đơn vị để thông báo ngay Công an tỉnh ghi nhận sự cố.

4.7. Thường xuyên cập nhật phần mềm diệt virus, hệ điều hành, phần mềm chuyên dụng... theo sự hướng dẫn của Công an tỉnh Quảng Nam.

4.8. Quản lý hệ thống phần mềm kết nối vào Hệ thống Cơ sở dữ liệu quốc gia về dân cư:

- Các hệ thống thông tin kết nối Cơ sở dữ liệu quốc gia về dân cư phải đảm bảo các điều kiện về an ninh, an toàn mạng theo quy định của Bộ công an, Bộ Thông tin và Truyền thông, có hồ sơ đề xuất cấp độ được thẩm định và phê duyệt, triển khai đầy đủ phương án đảm bảo an toàn Hệ thống thông tin theo cấp độ.

- Phải có phương án đảm bảo an toàn thông tin đáp ứng các yêu cầu an toàn cấp độ 3 trở lên theo quy định tại Điều 19 Nghị định số 85/2016/NĐ-CP của Chính phủ, Thông tư số 12/2012/TT-BTTTT của Bộ Thông tin và Truyền thông và tiêu chuẩn Quốc gia TCVN 11930:2017 về Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn Hệ thống thông tin theo cấp độ.

- Hệ thống thông tin phải được kiểm tra, đánh giá an toàn thông tin bởi các cơ quan, đơn vị chức năng của Bộ Công an, Bộ Thông tin và Truyền Thông trước khi kết nối, chia sẽ dữ liệu với Cơ sở dữ liệu quốc gia về dân cư và khi có thay đổi về thiết kế hệ thống.

4.9. Tuân thủ nghiêm, đầy đủ các yêu cầu và bảo mật an toàn thông tin. Chỉ cán bộ có tài khoản mới được khai thác thông tin từ cơ sở dữ liệu và phải thực hiện đúng quyền, nghĩa vụ theo quy định.

4.10. Cán bộ đăng ký tài khoản chỉ sử dụng dữ liệu được khai thác từ hệ thống đúng mục đích. Không thực hiện các hành vi cố ý gây thiệt hại, mất mát, lộ lọt thông tin trong hệ thống. Không tự ý truy cập hệ thống, thực hiện các chức

năng nằm ngoài quyền hạn khai thác, tấn công hoặc lợi dụng các vấn đề, điểm yếu an ninh trong kết nối hệ thống.

4.11. Có trách nhiệm bảo vệ các thông tin trong khi sử dụng, lưu trữ, truyền tải, trước các hành động truy cập sử dụng trái phép.

4.12. Có trách nhiệm đảm bảo an ninh an toàn cho những thông tin (dữ liệu, tài khoản...) nhận được, khai thác được từ hệ thống, đảm bảo không có cán bộ nào liên quan tiết lộ, sử dụng lưu trữ mô phỏng hoặc sao chép thông tin phục vụ cho mục đích cá nhân.

5. Quản lý sử dụng tài khoản/USB Token truy cập phần mềm hệ thống

5.1. Các tổ chức, cá nhân quản lý, sử dụng thiết bị, phần mềm đảm bảo an ninh, an toàn thông tin phải có bản cam kết đảm bảo An ninh an toàn và bảo mật thông tin trong kết nối đến Cơ sở dữ liệu quốc gia về dân cư.

5.2. Lãnh đạo các cơ quan, đơn vị, địa phương chịu trách nhiệm quản lý, phân công cán bộ trực tiếp sử dụng tài khoản/USB Token và áp dụng các biện pháp đảm bảo an ninh, an toàn thông tin dữ liệu hệ thống. Phân quyền truy cập cho cán bộ đăng ký tài khoản sử dụng dữ liệu được khai thác từ hệ thống để đảm bảo cán bộ sử dụng tài khoản không vượt quá quyền, chức năng, nhiệm vụ và tránh để xảy ra tình trạng tự ý truy cập hệ thống, thực hiện các chức năng nằm ngoài quyền hạn khai thác.

5.3. Cán bộ được phân công quản lý, sử dụng tài khoản quản trị (Admin) phải được thủ trưởng đơn vị trực tiếp giao bằng văn bản.

5.4. Cán bộ sử dụng phần mềm kết nối hệ thống có trách nhiệm:

- Quản lý tài khoản, mật khẩu sử dụng, thường xuyên thực hiện thay đổi mật khẩu tài khoản đảm bảo an ninh, an toàn thông tin, nghiêm cấm việc cung cấp tài khoản truy cập, cho người khác hoặc sử dụng tài khoản của người khác trái quy định.

- Không sử dụng tài khoản vượt quá quyền, chức năng nhiệm vụ. Trường hợp phát hiện cá nhân tổ chức sử dụng tài khoản với mục đích cá nhân kịp thời báo cáo lãnh đạo xử lý theo quy định.

- Sau khi sử dụng xong và không còn thao tác trên hệ thống, cán bộ tiến hành đăng xuất, thoát khỏi phiên làm việc, khóa thiết bị trước khi rời khỏi vị trí thiết bị.

- Lãnh đạo các cơ quan, đơn vị, địa phương thường xuyên kiểm tra việc quản lý tài khoản và sử dụng phần mềm thuộc hệ thống của cán bộ được giao nhiệm vụ đảm bảo an ninh, an toàn thông tin, xử lý các trường hợp để lộ lọt tài khoản mật khẩu và dữ liệu được lưu trữ trên hệ thống.

6. Quản lý dữ liệu đảm bảo an ninh, an toàn thông tin

6.1. Lãnh đạo các đơn vị, địa phương chịu trách nhiệm trực tiếp đảm bảo an ninh, an toàn thông tin, bảo mật dữ liệu liên quan đến thông tin công dân trên phần mềm, máy trạm, thiết bị lưu trữ thuộc hệ thống và chịu trách nhiệm theo quy định của Pháp luật nếu xảy ra vi phạm.

6.2. Cán bộ được giao tài khoản sử dụng truy cập hệ thống có trách nhiệm quản lý dữ liệu thuộc hệ thống. Cán bộ sử dụng khai thác dữ liệu thông tin hệ thống phải cam kết bảo vệ bí mật nhà nước và chịu trách nhiệm nếu để xảy ra sai phạm.

7. Kiểm tra giám sát

Thủ trưởng các cơ quan, đơn vị thường xuyên theo dõi, xây dựng kế hoạch kiểm tra định kỳ và đột xuất, trong đó thực hiện kiểm tra quá trình sử dụng thiết bị, phần mềm... đảm bảo an ninh, an toàn thông tin kết nối hệ thống.

Chương III
QUY ĐỊNH VỀ VIỆC KẾT NỐI, CHIA SẺ, KHAI THÁC THÔNG TIN VÀ BẢO VỆ DỮ LIỆU CÁ NHÂN TRONG CƠ SỞ DỮ LIỆU QUỐC GIA VỀ DÂN CƯ

Điều 6. Phương thức kết nối, chia sẻ thông tin giữa Cơ sở dữ liệu quốc gia về dân cư với Hệ thống thông tin giải quyết thủ tục hành chính cấp tỉnh và các hệ thống thông tin khác.

1. Việc kết nối, chia sẻ thông tin giữa Cơ sở dữ liệu quốc gia về dân cư với Hệ thống thông tin giải quyết thủ tục hành chính cấp tỉnh, Hệ thống thông tin khác được thực hiện thông qua nền tảng tích hợp, chia sẻ dữ liệu quốc gia, trục liên thông văn bản quốc gia, các nền tảng kết nối, tích hợp khác theo quy định của pháp luật.

2. Phương thức kết nối thông qua giao diện lập trình ứng dụng.

Điều 7. Điều kiện kết nối với Cơ sở dữ liệu quốc gia về dân cư.

1. Hệ thống thông tin của các cơ quan, tổ chức kết nối với Cơ sở dữ liệu quốc gia về dân cư phải đáp ứng các yêu cầu bảo đảm an toàn hệ thống thông tin cấp độ 3 trở lên theo quy định pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Trước khi thực hiện kết nối hoặc sau khi thực hiện kết nối với Cơ sở dữ liệu quốc gia về dân cư mà hệ thống thông tin của các cơ quan, tổ chức có sự điều chỉnh, thay đổi về thiết kế hệ thống thì phải được kiểm tra, đánh giá an ninh, an toàn thông tin. Việc kiểm tra, đánh giá được tiến hành bằng các thiết bị, phần mềm nghiệp vụ của lực lượng Công an nhân dân; nội dung kiểm tra, đánh giá gồm:

2.1. Việc thiết lập cấu hình bảo mật trên thiết bị hệ thống, máy chủ, ứng dụng và cơ sở dữ liệu;

2.2. Phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống đối với thiết bị hệ thống, máy chủ và ứng dụng;

2.3. An toàn thông tin cho mã nguồn ứng dụng;

2.4. An ninh, an toàn phần cứng;

2.5. Việc ban hành các quy định, chính sách quản lý tài khoản, ra, vào khu vực máy chủ, quản lý mật khẩu các tài khoản quản trị, quản lý truy cập, các văn bản thỏa thuận về quyền, nghĩa vụ, trách nhiệm của chủ thể tham gia quản lý, vận hành, cung cấp dịch vụ đối với hệ thống thông tin.

3. Đối với các hệ thống thông tin của Bộ Quốc phòng quản lý, cơ quan quản lý Cơ sở dữ liệu quốc gia về dân cư Bộ Công an có trách nhiệm phối hợp, hướng dẫn đơn vị chuyên môn của Bộ Quốc phòng thực hiện việc đánh giá, kiểm tra an ninh, an toàn thông tin theo quy định tại khoản 2 Điều này.

4. Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao chủ trì, phối hợp với Cục Kỹ thuật nghiệp vụ, cơ quan quản lý Cơ sở dữ liệu quốc gia về dân cư Bộ Công an và đơn vị có liên quan thực hiện:

4.1. Kiểm tra, đánh giá an ninh, an toàn thông tin của hệ thống thông tin có yêu cầu kết nối với Cơ sở dữ liệu quốc gia về dân cư trước khi kết nối và có văn bản xác nhận việc bảo đảm an ninh, an toàn thông tin; trường hợp các hệ thống thông tin có yêu cầu kết nối với Cơ sở dữ liệu quốc gia về dân cư đã được kết nối với nền tảng định danh và xác thực điện tử thì không phải kiểm tra, đánh giá an ninh, an toàn thông tin theo quy định tại khoản 2 Điều này.

4.2. Kiểm tra, đánh giá đột xuất việc bảo đảm an ninh, an toàn thông tin của hệ thống thông tin kết nối với Cơ sở dữ liệu quốc gia về dân cư theo nội dung quy định tại khoản 2 Điều này.

4.3. Kiểm tra, đánh giá định kỳ (01 lần trong 01 năm) bảo đảm an ninh, an toàn thông tin của hệ thống thông tin kết nối với Cơ sở dữ liệu quốc gia về dân cư theo nội dung quy định tại khoản 2 Điều này; trừ hệ thống thông tin do Bộ Quốc phòng quản lý; hệ thống thông tin đã được chia sẻ trực tuyến dữ liệu về giám sát an ninh mạng, an toàn thông tin cho Bộ Công an hoặc hệ thống thông tin đã được cơ quan có thẩm quyền tiến hành kiểm tra, đánh giá, xác nhận việc bảo đảm an ninh, an toàn không quá 01 năm theo quy định pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Điều 8. Quy trình thực hiện kết nối giữa Cơ sở dữ liệu quốc gia về dân cư với Hệ thống thông tin giải quyết thủ tục hành chính cấp tỉnh và các hệ thống thông tin khác.

1. Cơ quan, tổ chức quản lý hệ thống thông tin có văn bản đề nghị kết nối với Cơ sở dữ liệu quốc gia về dân cư gửi cơ quan quản lý Cơ sở dữ liệu quốc gia về dân cư Bộ Công an. Văn bản đề nghị kết nối gồm các nội dung sau: Đơn vị đăng ký; chức năng, nhiệm vụ, quyền hạn được giao; tên hệ thống thông tin, cơ sở dữ liệu đề nghị được kết nối, chia sẻ; thông tin cán bộ phụ trách kết nối, chia sẻ và khai thông tin; mục đích, phạm vi, nội dung thông tin, số lượng trường thông tin cần chia sẻ; dịch vụ đăng ký sử dụng trong Cơ sở dữ liệu quốc gia về dân cư, tài liệu mô tả kỹ thuật thành phần hệ thống có kết nối với Cơ sở dữ liệu quốc gia về dân cư.

2. Ngay sau khi nhận được văn bản đề nghị, cơ quan quản lý Cơ sở dữ liệu quốc gia về dân cư Bộ Công an thực hiện:

2.1. Cung cấp tài liệu kỹ thuật phục vụ kết nối, chia sẻ, khai thác thông tin trong Cơ sở dữ liệu quốc gia về dân cư cho cơ quan, tổ chức có đề nghị kết nối.

2.2. Hỗ trợ các cơ quan, tổ chức thực hiện kết nối, điều chỉnh phần mềm và kiểm thử kỹ thuật các dịch vụ chia sẻ, khai thác thông tin trong Cơ sở dữ liệu quốc gia về dân cư.

2.3. Phối hợp với Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao, Cục Kỹ thuật nghiệp vụ thuộc Bộ Công an và đơn vị có liên quan tiến hành kiểm tra, đánh giá việc bảo đảm an ninh, an toàn thông tin hệ thống thông tin của cơ quan, tổ chức có đề nghị kết nối.

Điều 9. Lưu trữ nhật ký kết nối, chia sẻ, khai thác thông tin.

1. Cơ quan quản lý Cơ sở dữ liệu quốc gia về dân cư Bộ Công an và cơ quan, tổ chức có các hoạt động kết nối, chia sẻ và khai thác thông tin với Cơ sở dữ liệu quốc gia về dân cư có trách nhiệm lưu lại nhật ký thực hiện kết nối, chia sẻ, khai thác thông tin để phục vụ công tác theo dõi, kiểm tra, giám sát.

2. Thời hạn tối thiểu lưu trữ nhật ký về kết nối, chia sẻ, khai thác thông tin trong hệ thống Cơ sở dữ liệu quốc gia về dân cư là 02 năm kể từ thời điểm thực hiện việc kết nối, chia sẻ, khai thác thông tin.

Điều 10. Nguyên tắc bảo vệ thông tin dữ liệu cá nhân và khai thác sử dụng thông tin, dữ liệu cá nhân, xử lý vi phạm quy định bảo vệ dữ liệu cá nhân.

1. Cá nhân bảo vệ thông tin, dữ liệu cá nhân của mình và tuân thủ quy định của pháp luật về cung cấp thông tin, dữ liệu cá nhân khi sử dụng dịch vụ trong hệ thống cơ sở dữ liệu quốc gia về dân cư. Dữ liệu cá nhân được xử lý theo quy định của pháp luật.

2. Cơ quan, tổ chức, cá nhân xử lý thông tin, dữ liệu cá nhân có trách nhiệm bảo đảm an toàn thông tin đối với thông tin, dữ liệu do mình xử lý phải xây dựng và công bố công khai biện pháp xử lý, bảo vệ thông tin, dữ liệu cá nhân của tổ chức, cá nhân mình.

3. Không được cung cấp, chia sẻ, thông tin, dữ liệu cá nhân mà mình đã khai thác, sử dụng cho bên thứ ba, trừ trường hợp có sự đồng ý của chủ thể thông tin, dữ liệu cá nhân đó hoặc theo yêu cầu của cơ quan nhà nước có thẩm quyền.

4. Dữ liệu cá nhân được áp dụng các biện pháp bảo vệ, bảo mật trong quá trình xử lý, bao gồm cả việc bảo vệ trước các hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân và phòng, chống sự mất mát, phá hủy hoặc thiệt hại do sự cố, sử dụng các biện pháp kỹ thuật.

5. Cơ quan, tổ chức, cá nhân vi phạm quy định bảo vệ dữ liệu cá nhân tùy theo mức độ có thể bị xử lý kỷ luật, xử phạt vi phạm hành chính, xử lý hình sự theo quy định.

Điều 11. Bảo đảm an toàn thông tin, dữ liệu cá nhân, hành vi bị nghiêm cấm

1. Tổ chức, cá nhân xử lý thông tin, dữ liệu cá nhân phải áp dụng biện pháp quản lý, kỹ thuật phù hợp để bảo vệ thông tin, dữ liệu cá nhân do mình thu thập, lưu trữ; tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật và bảo đảm an toàn thông tin.

2. Khi xảy ra hoặc có nguy cơ xảy ra sự cố an toàn thông tin, tổ chức, cá nhân xử lý thông tin, dữ liệu cá nhân cần áp dụng biện pháp khắc phục, ngăn chặn trong thời gian sớm nhất.

3. Xử lý dữ liệu cá nhân trái với quy định của pháp luật về bảo vệ dữ liệu cá nhân.

4. Xử lý dữ liệu cá nhân để tạo ra thông tin, dữ liệu nhằm chống lại nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam.

5. Xử lý dữ liệu cá nhân để tạo ra thông tin, dữ liệu gây ảnh hưởng tới an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân khác.

6. Cản trở hoạt động bảo vệ dữ liệu cá nhân của cơ quan có thẩm quyền.

7. Lợi dụng hoạt động bảo vệ dữ liệu cá nhân để vi phạm pháp luật.

Chương IV
TRÁCH NHIỆM CỦA CÁC TỔ CHỨC CÁ NHÂN VÀ KHEN THƯỞNG, XỬ LÝ VI PHẠM

Điều 12. Trách nhiệm của các tổ chức cá nhân

1. Tuyên truyền, nâng cao nhận thức cho Lãnh đạo, cán bộ, công nhân viên chức tại các cơ quan, đơn vị về đảm bảo an ninh, an toàn thông tin theo quy định của Luật Bảo vệ bí mật nhà nước.

2. Thủ trưởng các cơ quan, đơn vị chịu trách nhiệm chỉ đạo, rà soát, nâng cao hạ tầng Công nghệ thông tin của đơn vị đảm bảo các yêu cầu về an toàn an ninh mạng; xây dựng hồ sơ đề xuất cấp độ an toàn thông tin đối với các hệ thống được giao chủ quản và tổ chức triển khai theo hồ sơ được duyệt; ban hành quy chế đảm bảo an toàn thông tin tại đơn vi, chịu trách nhiệm trước Trưởng Ban chỉ đạo về vấn đề quản lý, sử dụng vận hành hệ thống của cơ quan, đơn vị khi kết nối vào hệ thống thuộc Đề án 06.

3. Thường xuyên kiểm tra, đề xuất kiểm tra an ninh, an toàn thông tin; phối hợp với các đơn vị có liên quan trong Công an tỉnh và Sở Thông tin và Truyền thông để kiểm tra an ninh, an toàn thông tin xử lý các sự cố có liên quan.

Điều 13. Khen thưởng và xử lý vi phạm

1. Cơ quan đơn vị, cá nhân có thành tích trong việc thực hiện Đề án 06 thì được khen thưởng theo quy định của Pháp luật.

2. Nếu vi phạm Quy định này và các quy định khác của Pháp luật trong việc tham gia thực hiện Đề án 06 thì tùy theo tính chất, mức độ, hậu quả của sai phạm sẽ bị xử lý kỷ luật, vi phạm hành chính hoặc truy cứu trách nhiệm hình sự theo quy định của pháp luật.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 14. Trách nhiệm thi hành

1. Căn cứ vào nội dung Quy định này, lãnh đạo các cơ quan, đơn vị, địa phương khẩn trương tổ chức thực hiện các phần công việc được phân công, kịp thời tháo gỡ những khó khăn, vướng mắc, phát hiện sơ hở, thiếu sót trong việc đảm bảo an ninh, an toàn thông tin các thiết bị kết nối hệ thống.

2. Sở Thông tin và Truyền thông tỉnh xây dựng tài liệu hướng dẫn sử dụng, thực hiện các dịch vụ khai thác thông tin trong Cơ sở dữ liệu quốc gia về dân cư và các hệ thống thông tin khác với hệ thống thông tin giải quyết thủ tục hành chính trên địa bàn tỉnh Quảng Nam; quá trình thao tác, sử dụng các chức năng, thực hiện kết nối, chia sẻ giữa các hệ thống thông tin, nếu phát sinh sự cố cần xử lý, hỗ trợ,

giải đáp vướng mắc các cơ quan, tổ chức, các nhân liên hệ Sở Thông tin và Truyền thông để thực hiện.

3. Công an tỉnh chủ trì, phối hợp với Sở Thông tin và Truyền thông và các đơn vị có liên quan thành lập Đoàn kiểm tra, định kỳ kiểm tra tại các đơn vị, địa phương theo kế hoạch; theo dõi, hướng dẫn, kiểm tra việc chấp hành quy định này, kết quả kiểm tra các quy định phải đánh giá ưu điểm, hạn chế, phát hiện những sơ hở, thiếu sót, lỗ hổng và kiến nghị các biện pháp khắc phục, xử lý kỷ luật *(nếu có)* và được thể hiện bằng văn bản. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, kịp thời báo cáo Ủy ban nhân dân tỉnh *(qua Công an tỉnh*) để theo dõi, chỉ đạo hoặc điều chỉnh, bổ sung cho phù hợp./.