ỦY BAN NHÂN DÂN TỈNH AN GIANG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 59/2024/QĐ-UBND	*An Giang, ngày 27 tháng 12 năm 2024*

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động của các cơ quan Nhà nước trên địa bàn tỉnh An Giang

ỦY BAN NHÂN DÂN TỈNH AN GIANG

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19 tháng 6 năm 2015; Luật Sửa đổi, bổ sung một số điều của Luật Tổ chức Chính phủ và Luật Tổ chức chính quyền địa phương ngày 22 tháng 11 năm 2019;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật ngày 22 tháng 6 năm 2015; Luật Sửa đổi, bổ sung một số điều của Luật Ban hành văn bản quy phạm pháp luật ngày 18 tháng 6 năm 2020;

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Luật Bảo vệ bí mật nhà nước ngày 15 tháng 11 năm 2018;

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

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Nghị định số 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 của Chính phủ quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng;

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 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ về bảo vệ dữ liệu cá nhân;

Căn cứ Nghị định số 69/2024/NĐ-CP ngày 25 tháng 6 năm 2024 của Chính phủ quy định về định danh và xác thực điện tử;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ ban hành Quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Thông tư số 24/2020/TT-BTTTT ngày 09 tháng 9 năm 2020 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về công tác triển khai, giám sát công tác triển khai và nghiệm thu dự án đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước;

Căn cứ Thông tư số 19/2021/TT-BTTTT ngày 03 tháng 12 năm 2021 của Bộ trưởng Bộ Thông tin và Truyền thông ban hành Danh mục sản phẩm công nghệ thông tin trọng điểm;

Căn cứ Thông tư số 08/2023/TT-BTTTT ngày 28 tháng 7 năm 2023 của Bộ trưởng Bộ Thông tin và Truyền thông hướng dẫn về vị trí việc làm lãnh đạo, quản lý và chức danh nghề nghiệp viên chức chuyên ngành; cơ cấu viên chức theo chức danh nghề nghiệp trong đơn vị sự nghiệp công lập thuộc ngành, lĩnh vực thông tin và truyền thông;

Căn cứ Thông tư số 09/2023/TT-BTTTT ngày 28 tháng 7 năm 2023 của Bộ trưởng Bộ Thông tin và Truyền thông hướng dẫn về vị trí việc làm công chức nghiệp vụ chuyên ngành Thông tin và Truyền thông trong cơ quan, tổ chức thuộc ngành, linh vực Thông tin và Truyền thông;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về việc bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 46/2022/TT-BCA ngày 04 tháng 11 năm 2022 của Bộ trưởng Bộ Công an quy định về việc 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;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 141/TTr-STTTT ngày 05 tháng 11 năm 2024.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin mạng trong hoạt động của các cơ quan Nhà nước trên địa bàn tỉnh An Giang.

Điều 2. Điều khoản thi hành

1. Quyết định này có hiệu lực thi hành kể từ ngày 08 tháng 01 năm 2025.

2. Quyết định này thay thế Quyết định số 67/2017/QĐ-UBND ngày 04 tháng 10 năm 2017 của Ủy ban nhân dân tỉnh ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh An Giang; Quyết định số 61/2018/QĐ-UBND ngày 27 tháng 12 năm 2018 của Ủy ban nhân dân tỉnh sửa đổi, bổ sung một số điều của Quy chế ban hành kèm theo Quyết định số 67/2017/QĐ-UBND.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh; Giám đốc Sở Thông tin và Truyền thông; Thủ trưởng các Sở, ban, ngành tỉnh; Chủ tịch Ủy ban nhân dân huyện, thị xã, thành phố; các cơ quan, đơn vị và cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

***Nơi nhận*:**
- Bộ Thông tin và Truyền thông;
- Cục Kiểm tra văn bản QPPL - Bộ Tư pháp;
- TT: TU, HĐND tỉnh, UBND tỉnh;
- UBMTTQ VN tỉnh;
- VP.TU, các Ban đảng;
- Sở, ban, ngành, đoàn thể tỉnh;
- UBND huyện, thị xã, thành phố;
- Cơ quan Báo, Đài tỉnh;
- Trung tâm Công báo – Tin học;
- Cổng thông tin điện tử tỉnh;
- Phòng: KGVX, TH;
- Lưu: VT.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Hồ Văn Mừng

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

QUY CHẾ
Bảo đảm an toàn thông tin mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh An Giang

(Kèm theo Quyết định 59/2024/QĐ-UBND ngày 27 tháng 12 năm 2024 của Ủy ban nhân dân tỉnh An Giang)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định các nội dung, trách nhiệm và công tác bảo đảm an toàn thông tin (gọi tắt là ATTT) mạng cho các hệ thống thông tin trong hoạt động chuyển đổi số của các cơ quan nhà nước trên địa bàn tỉnh.

Điều 2. Đối tượng áp dụng

1. Sở, ban, ngành tỉnh; UBND huyện, thị xã, thành phố; UBND xã, phường, thị trấn trên địa bàn tỉnh; các đơn vị sự nghiệp trực thuộc Ủy ban nhân dân (UBND) tỉnh; các đơn vị sự nghiệp trực thuộc các sở, ngành tỉnh; đơn vị thuộc UBND cấp huyện (gọi tắt là các cơ quan, đơn vị).

2. Cán bộ, công chức, viên chức (gọi tắt là CCVC), người lao động và các tổ chức, cá nhân có liên quan tham gia vận hành, khai thác các hệ thống thông tin tại cơ quan, đơn vị quy định tại khoản 1 Điều này.

3. Các cơ quan, tổ chức, doanh nghiệp, cá nhân cung cấp dịch vụ công nghệ thông tin (CNTT), Internet, ATTT mạng hoặc có tham gia vào các hoạt động chuyển đổi số của các cơ quan, đơn vị thuộc khoản 1 Điều này.

Điều 3. Giải thích từ ngữ

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

1. An toàn thông tin mạng theo quy định tại khoản 1 Điều 3 của Luật An toàn thông tin mạng số 86/2015/QH13.

2. Mạng theo quy định tại khoản 2 Điều 3 của Luật An toàn thông tin mạng.

3. Hệ thống thông tin theo quy định tại khoản 3 Điều 3 của Luật An toàn thông tin mạng.

4. Xâm phạm ATTT mạng theo quy định tại khoản 6 Điều 3 của Luật An toàn thông tin mạng.

5. Sự cố An toàn thông tin mạng theo quy định tại khoản 7 Điều 3 của Luật An toàn thông tin mạng.

6. Phần mềm độc hại theo quy định tại khoản 11 Điều 3 của Luật An toàn thông tin mạng.

7. Tấn công mạng theo quy định tại khoản 8 Điều 2 của Luật An ninh mạng số 24/2018/QH14.

8. Chủ quản hệ thống thông tin theo quy định tại khoản 1 Điều 3 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.

9. Đơn vị vận hành hệ thống thông tin theo quy định tại khoản 3 Điều 3 Nghị định số 85/2016/NĐ-CP.

10. Đơn vị chuyên trách về CNTT theo quy định tại khoản 4 Điều 3 Nghị định số 85/2016/NĐ-CP.

11. Đơn vị chuyên trách về ATTT theo quy định tại khoản 5 Điều 3 Nghị định số 85/2016/NĐ-CP.

12. Bộ phận chuyên trách về ATTT theo quy định tại khoản 6 Điều 3 Nghị định số 85/2016/NĐ-CP.

Bộ phận phụ trách về ATTT mạng là bộ phận do thủ trưởng cơ quan, đơn vị thành lập hoặc chỉ định để thực thi nhiệm vụ bảo đảm ATTT và ứng cứu sự cố ATTT mạng. Trường hợp cơ quan, đơn vị không có Bộ phận phụ trách về ATTT mạng thì nhân sự phụ trách về ATTT mạng thực hiện nhiệm vụ bảo đảm ATTT và ứng cứu sự cố ATTT mạng tại cơ quan, đơn vị.

13. Nhân sự phụ trách về ATTT mạng là CCVC, chuyên gia, người lao động đào tạo ngành CNTT hoặc tương đương, được giao nhiệm vụ quản lý, tham mưu về lĩnh vực ATTT mạng các cơ quan, đơn vị; có ít nhất 01 chứng chỉ hoặc chứng nhận được đào tạo về ATTT mạng (trường hợp chưa có chứng chỉ, chứng nhận thì phải được đào tạo, bồi dưỡng ngay sau đó, trong khoảng thời sau không quá 03 tháng kể từ khi được phân công).

14. Mật khẩu mạnh là mật khẩu có tối thiểu 08 ký tự, bao gồm sự kết hợp chữ hoa, chữ thường, số và ký tự đặc biệt.

Điều 4. Nguyên tắc bảo đảm An toàn thông tin mạng

Thực hiện theo quy định tại Điều 4 Luật An toàn thông tin mạng.

Điều 5. Các hành vi bị nghiêm cấm và xử lý vi phạm về ATTT mạng

1. Các hành vi bị nghiêm cấm về an toàn, an ninh thông tin mạng quy định tại Điều 7 Luật ATTT mạng; Điều 8 Luật An ninh mạng; Điều 5 Luật Bảo vệ bí mật nhà nước số 29/2018/QH14.

2. Xử lý vi phạm pháp luật về ATTT mạng theo quy định tại Điều 8 Luật An toàn thông tin mạng.

Chương II
QUY ĐỊNH VỀ BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 6. Bảo vệ dữ liệu cá nhân

1. CCVC, người lao động có trách nhiệm tự bảo vệ thông tin cá nhân của mình và tuân thủ các quy định tại khoản 1, khoản 2 Điều 10; khoản 1, khoản 4 Điều 16; khoản 3 Điều 17; khoản 1 Điều 18 Luật An toàn thông tin mạng và văn bản pháp luật có liên quan.

2. Khi sử dụng, khai thác các hệ thống thông tin của cơ quan, đơn vị trên địa bàn tỉnh, có trách nhiệm:

a) Tự quản lý và chịu trách nhiệm về bảo vệ thông tin cá nhân đã được khai báo trong các hệ thống thông tin; không tiết lộ tài khoản đăng nhập, đấu nối, truy cập trái phép vào các phần mềm dùng chung của tỉnh. Thực hiện bảo mật tài khoản truy cập các hệ thống, không chia sẻ tài khoản, mật khẩu, thông tin cá nhân với người khác nếu trường hợp bận công tác thì phải có giấy ủy quyền việc quản lý, sử dụng tài khoản ghi rõ thời gian ủy quyền, nêu rõ trách nhiệm của các bên.

b) Phải thực hiện việc đổi mật khẩu mạnh ngay sau khi được cấp tài khoản truy cập vào các phần mềm dùng chung của tỉnh, cơ quan, đơn vị; Thực hiện cơ chế xác thực hai hay nhiều yếu tố xác thực khi đăng nhập (nếu hệ thống có hỗ trợ tính năng), định kỳ thay đổi mật khẩu ít nhất 06 tháng một lần.

c) Khi khai thác, sử dụng các phần mềm dùng chung của tỉnh tại các điểm truy cập internet công cộng, phải bảo đảm sử dụng tiêu chuẩn kết nối giao thức truyền tải siêu văn bản (HTTPS - HyperText Transfer Protocol Secure) khi đăng nhập các tài khoản, tuyệt đối không đặt chế độ lưu trữ mật khẩu trong quá trình sử dụng.

3. Các cơ quan, đơn vị, cá nhân khi xử lý thông tin cá nhân phải tuân thủ đầy đủ các nội dung theo quy định tại khoản 2, 3, 4, 5 Điều 16; khoản 1, 2 Điều 17; khoản 3 Điều 18; Điều 19 của Luật ATTT mạng và các quy định sau:

a) Quản lý và phân quyền truy cập trong các phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ, quyền hạn của người tham gia quản lý, vận hành, khai thác, sử dụng các phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu.

b) Khi CCVC, người lao động đã nghỉ việc hoặc chuyển công tác, các cơ quan, đơn vị phải thực hiện việc thu hồi các máy móc, thiết bị CNTT liên quan theo quy định; đồng thời phải thông báo ngay bằng văn bản đến cơ quan quản lý, quản trị nền tảng, phần mềm ứng dụng, hệ thống thông tin, cơ sở dữ liệu để thực hiện các biện pháp kỹ thuật cập nhật lại, khóa hoặc hủy tài khoản người dùng.

c) Việc cấp phát, đóng, khóa tài khoản CCVC, người lao động có quyền tra cứu thông tin trên Cơ sở dữ liệu quốc gia về dân cư liên quan đến các hệ thống thông tin, nền tảng ứng dụng dùng chung của tỉnh An Giang:

- Các cơ quan, đơn vị có văn bản gửi Sở Thông tin và Truyền thông để tổng hợp gửi Phòng Cảnh sát quản lý hành chính về trật tự xã hội (PC06) – Công an tỉnh An Giang khi có thông tin liên quan đến việc thêm mới, đóng, khóa tài khoản có quyền tra cứu thông tin công dân.

- CCVC, người lao động thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu thì trong vòng không quá 05 ngày làm việc, cơ quan, đơn vị quản lý CCVC, người lao động đó phải thông báo cho cơ quan, đơn vị chủ quản hệ thống thông tin để điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng trên hệ thống thông tin, nền tảng ứng dụng dùng chung của tỉnh.

4. Sở Thông tin và Truyền thông, Công an tỉnh thực hiện công tác quản lý nhà nước về bảo vệ thông tin cá nhân trên mạng theo các nội dung quy định tại Điều 20 của Luật ATTT mạng, Điều 29 của Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ về bảo vệ dữ liệu cá nhân.

5. Thực hiện các hoạt động bảo vệ dữ liệu cá nhân theo quy định tại Chương II Nghị định số 13/2023/NĐ-CP.

Điều 7. Bảo đảm an toàn hệ thống thông tin theo cấp độ

1. Người đứng đầu cơ quan, đơn vị trực tiếp chỉ đạo và phụ trách công tác bảo đảm ATTT mạng; chịu trách nhiệm trước pháp luật và Chủ tịch UBND tỉnh nếu để hệ thống thông tin thuộc phạm vi quản lý không bảo đảm ATTT mạng, để xảy ra sự cố nghiêm trọng.

2. Việc đảm bảo an toàn hệ thống thông tin theo cấp độ trong hoạt động của cơ quan, đơn vị phải được thực hiện thường xuyên, liên tục từ khâu thiết kế, xây dựng, vận hành đến khi hủy bỏ; tuân thủ theo tiêu chuẩn, quy chuẩn kỹ thuật của Bộ Thông tin và Truyền thông và các quy định có liên quan khác.

3. Chủ quản hệ thống thông tin có trách nhiệm chỉ đạo, tổ chức thực hiện phương án đảm bảo an toàn hệ thống thông tin theo cấp độ theo quy định tại Nghị định số 85/2016/NĐ-CP.

4. Đơn vị vận hành hệ thống thông tin thực hiện xác định cấp độ và lập hồ sơ đề xuất cấp độ trình cấp có thẩm quyền phê duyệt, đồng thời triển khai kịp thời các phương án đảm bảo ATTT theo hồ sơ cấp độ đã được phê duyệt.

5. Hệ thống thông tin khi được đầu tư xây dựng mới hoặc mở rộng, nâng cấp cần được kiểm thử về tính an toàn, bảo mật trước khi nghiệm thu, bàn giao đưa vào khai thác, sử dụng theo quy định tại điểm b khoản 3 Điều 10 Thông tư số 24/2020/TT-BTTTT ngày 09 tháng 9 năm 2020 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về công tác triển khai, giám sát công tác triển khai và nghiệm thu dự án đầu tư ứng dụng CNTT sử dụng nguồn vốn ngân sách nhà nước.

6. Lưu trữ nhật ký kết nối, chia sẻ, khai thác thông tin với Cơ sở dữ liệu quốc gia về dân cư tuân thủ theo quy định tại khoản 2 Điều 8 Thông tư số 46/2022/TT-BCA ngày 04 tháng 11 năm 2022 của Bộ trưởng Bộ Công an quy định về việc 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.

7. Hệ thống thông tin có kết nối, chia sẻ và khai thác thông tin với Cơ sở dữ liệu quốc gia về dân cư phải bảo đảm các cơ chế: xác thực đăng nhập; yêu cầu người dùng đặt mật khẩu mạnh; việc thay đổi mật khẩu mặc định, mật khẩu đăng nhập lần đầu không được trùng với mật khẩu mặc định; sau 05 lần đăng nhập mật khẩu không thành công thì hệ thống tự động khóa tài khoản người dùng; mật khẩu được yêu cầu thay đổi định kỳ ít nhất 06 tháng một lần; ngăn chặn tấn công vét cạn mật khẩu (mã Captcha); xác thực đăng nhập 02 lớp hoặc nhiều yếu tố xác thực khi đăng nhập; ghi nhận dấu hiệu bất thường liên quan đến việc sử dụng tài khoản người dùng, quản trị khai thác dữ liệu hệ thống và quy định pháp luật.

Điều 8. Quản lý thuê dịch vụ CNTT

1. Xác định rõ phạm vi, trách nhiệm, quyền hạn và nghĩa vụ của các bên về bảo đảm ATTT khi ký kết hợp đồng thuê. Trong hợp đồng phải bao gồm các điều khoản về việc xử lý vi phạm quy định bảo đảm ATTT và trách nhiệm bồi thường thiệt hại do hành vi vi phạm của bên cung cấp dịch vụ gây ra.

2. Cơ quan, đơn vị chủ trì thuê dịch vụ CNTT phải có trách nhiệm

a) Quản lý chặt chẽ thông tin, dữ liệu phát sinh từ dịch vụ thuê, không cho phép bên cung cấp dịch vụ truy nhập, sử dụng thông tin, dữ liệu thuộc phạm vi Nhà nước quản lý.

b) Yêu cầu bên cung cấp dịch vụ phải bảo mật thông tin, dữ liệu, mã nguồn, tài liệu thiết kế; triển khai các biện pháp bảo đảm ATTT theo quy định tại Quy chế này, Luật ATTT mạng và các quy định khác có liên quan.

c) Giám sát chặt chẽ và giới hạn quyền truy cập của bên cung cấp dịch vụ khi cho phép truy cập vào hệ thống thông tin của cơ quan, đơn vị.

d) Khi phát hiện bên cung cấp dịch vụ có dấu hiệu vi phạm quy định bảo đảm ATTT phải tạm dừng hoặc đình chỉ hoạt động của bên cung cấp dịch vụ tùy theo mức độ vi phạm; thông báo chính thức các hành vi vi phạm của bên cung cấp dịch vụ cho cơ quan chức năng để phối hợp xử lý vi phạm theo quy định pháp luật; thu hồi ngay lập tức quyền truy cập hệ thống thông tin đã cấp cho bên cung cấp dịch vụ; kiểm tra, xác định, lập báo cáo mức độ vi phạm và thiệt hại xảy ra, thông báo cho bên cung cấp dịch vụ và tiến hành các thủ tục xử lý vi phạm và bồi thường thiệt hại.

đ) Yêu cầu bên cung cấp dịch vụ phải có trách nhiệm lập hồ sơ ATTT theo cấp độ được quy định tại Nghị định số 85/2016/NĐ-CP.

e) Yêu cầu bên cung cấp dịch vụ phải đảm bảo khả năng kết nối, mở rộng, chia sẻ dữ liệu với các hệ thống thông tin dùng chung của tỉnh; tuân thủ Kiến trúc chính quyền điện tử tỉnh An Giang; Khung kiến trúc chính phủ điện tử Việt Nam hiện hành.

3. Trách nhiệm của cơ quan, đơn vị chủ trì thuê khi kết thúc hợp đồng sử dụng dịch vụ

a) Thu hồi quyền truy cập hệ thống thông tin và các tài sản khác liên quan đã cấp cho bên cung cấp dịch vụ; thay đổi các khóa, mật khẩu truy cập hệ thống thông tin.

b) Yêu cầu bên cung cấp dịch vụ chuyển giao đầy đủ các thông tin, dữ liệu, mã nguồn, tài liệu thiết kế và các công cụ cần thiết để bảo đảm cơ quan, đơn vị vẫn có thể khai thác sử dụng dịch vụ được liên tục kể cả trong trường hợp thay đổi bên cung cấp dịch vụ.

4. Đơn vị cung cấp dịch vụ khi có thay đổi về mặt hệ thống, ứng dụng, mã nguồn và chức năng hệ thống phần mềm phục vụ kết nối cơ sở dữ liệu quốc gia về dân cư cần báo cáo về Sở Thông tin và Truyền thông để tổng hợp báo cáo Tổ chức có liên quan về triển khai và đảm bảo an toàn cơ sở dữ liệu quốc gia về dân cư trên địa bàn tỉnh để phối hợp đơn vị nghiệp vụ Bộ Công an, Bộ Thông tin và Truyền thông thực hiện kiểm tra an ninh, ATTT đảm bảo đáp ứng các tiêu chí theo hướng dẫn của Bộ Công an, Bộ Thông tin và Truyền thông và quy định pháp luật.

5. Có phương án hợp đồng chặt chẽ với nhà cung cấp dịch vụ và có cơ chế quản lý đối với các tài khoản thuộc các hệ thống thuê dịch vụ hạ tầng của nhà cung cấp dịch vụ, tránh tình trạng ủy quyền toàn bộ việc quản trị, vận hành hệ thống cho nhà cung cấp dịch vụ liên quan đến khai thác, sử dụng cơ sở dữ liệu quốc gia về dân cư.

Điều 9. Bảo vệ bí mật nhà nước trong hoạt động chuyển đổi số

1. Quy định về soạn thảo, in ấn, phát hành và sao, chụp tài liệu mật

a) Không được soạn thảo, lưu giữ, chuyển giao, đăng tải, phát hành thông tin, có chứa nội dung bí mật nhà nước trên máy tính hoặc thiết bị khác đã kết nối hoặc đang kết nối với mạng Internet, mạng máy tính, mạng viễn thông, trừ trường hợp lưu giữ bí mật nhà nước theo quy định của pháp luật về cơ yếu.

b) Không được in, sao, chụp tài liệu bí mật nhà nước trên các thiết bị kết nối mạng Internet, mạng máy tính, mạng viễn thông.

c) Phải bố trí ít nhất 01 máy tính độc lập riêng, không kết nối mạng nội bộ và mạng Internet và được bảo quản theo chế độ mật, dùng để quản lý, soạn thảo, lưu trữ các văn bản, tài liệu mật của nhà nước theo quy định.

2. Khi sửa chữa, khắc phục sự cố của máy tính dùng soạn thảo văn bản mật, các phòng, đơn vị phải báo cáo cho người có thẩm quyền. Không được cho phép các tổ chức, cá nhân không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

3. Trước khi thanh lý, chuyển mục đích sử dụng các máy tính hoặc các thiết bị khác trong các cơ quan nhà nước có mang thông tin mật, phải dùng các biện pháp kỹ thuật xoá bỏ vĩnh viễn dữ liệu bí mật nhà nước trên các thiết bị.

Điều 10. Bảo đảm an toàn dữ liệu

1. Quản lý tài khoản và chữ ký số

a) Khi được cấp tài khoản, chữ ký số lần đầu cho người dùng truy nhập, người dùng phải thay đổi mật khẩu sau khi đăng nhập thành công lần đầu; chủ tài khoản,

chữ ký số không chia sẻ, không giao quyền tài khoản, không giao chứng thư chữ ký số và mật khẩu truy nhập cho người khác.

b) Các Cổng/Trang thông tin điện tử phải được cấu hình truy cập sử dụng theo tiêu chuẩn kết nối giao thức truyền tải siêu văn bản (HTTPS - HyperText Transfer Protocol Secure). Các hệ thống thông tin khi phân quyền phải thiết lập chế độ giới hạn số lần đăng nhập không hợp lệ vào hệ thống tối đa không quá 05 lần, khi người dùng đăng nhập sai vượt quá số lần quy định, tài khoản chuyển sang chế độ khóa quyền truy cập; các hệ thống thông tin xác lập chế độ thoát ra khỏi hệ thống nếu người sử dụng không tương tác trên hệ thống của phiên làm việc quá 10 phút.

c) Tài khoản thư điện tử công vụ (https://mail.angiang.gov.vn), chữ ký số chuyên dùng công vụ chỉ phục vụ cho các hoạt động mang tính công vụ, không sử dụng để giao dịch, đăng ký trên mạng xã hội, các trang thông tin điện tử công cộng khác.

2. Đối với các dữ liệu quan trọng, các cơ quan, đơn vị cần lên phương án sao lưu dự phòng theo phương án sao lưu tối thiểu theo quy tắc 3-2-1, bao gồm: giữ ít nhất ba bản sao dữ liệu, lưu trữ hai bản sao trên các phương tiện lưu trữ khác nhau, lưu trữ một bản sao lưu ngoại vi. Các cơ quan, đơn vị khi thuê dịch vụ cần yêu cầu nhà cung cấp dịch vụ thiết lập các giải pháp sao lưu tự động đối với dữ liệu trên máy chủ cơ sở dữ liệu và máy chủ ứng dụng và xây dựng các kịch bản có sẵn để khôi phục lại toàn bộ máy chủ hoặc các tập tin, thư mục khi xảy ra sự cố. Dữ liệu sao lưu phải được lưu trữ an toàn trên Hệ thống lưu trữ dự phòng, thiết bị lưu trữ ngoài và được kiểm tra thường xuyên đảm bảo sẵn sàng cho việc sử dụng khi cần; việc kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu tối thiểu 6 tháng một lần (hoặc khi có yêu cầu đột xuất).

3. Tên miền phục vụ cho tổ chức, cơ quan chính phủ trên địa bàn tỉnh (*.angiang.gov.vn) khi không còn sử dụng, các cơ quan, đơn vị có văn bản gửi đến Sở Thông tin và Truyền thông để đề nghị thu hồi tên miền; các hệ thống thông tin không sử dụng, chủ quản hệ thống thông tin thực hiện việc thu hồi máy chủ, thu hồi ứng dụng và thực hiện việc lưu trữ dữ liệu ra thiết bị lưu trữ ngoài và yêu cầu cơ quan, đơn vị cung cấp dịch vụ lưu ký xóa hoàn toàn dữ liệu trên các máy chủ.

4. Cơ quan, đơn vị quản lý máy chủ, máy trạm và thiết bị lưu trữ khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài cơ quan, đơn vị phải tháo rời bộ phận lưu trữ khỏi thiết bị và để lại cơ quan, đơn vị hoặc xóa dữ liệu lưu trữ trên thiết bị. Trường hợp thiết bị lưu trữ cần bảo hành, bảo dưỡng, sửa chữa phải sao lưu dữ liệu trên thiết bị sang thiết bị lưu trữ khác khoặc xóa dữ liệu lưu trữ trên thiết bị. Khi thanh lý thiết bị phải xóa dữ liệu lưu trữ bằng phần mềm hoặc thiết bị hủy dữ liệu chuyên dụng.

5. Thông tin, dữ liệu thuộc phạm vi bí mật Nhà nước phải được quản lý theo quy định hiện hành về bảo vệ bí mật Nhà nước.

Điều 11. Bảo đảm an toàn thiết bị đầu cuối

1. CCVC, người lao động sử dụng máy tính để xử lý công việc phải tuân thủ các quy định sau:

a) Phải thiết lập chế độ tự động cập nhật hệ điều hành trên máy tính, phải thiết lập mật khẩu truy nhập chế độ tự động bảo vệ màn hình khi không sử dụng; sử dụng những trình duyệt an toàn, đáng tin cậy, cài đặt phần mềm phòng chống mã độc; thiết lập chế độ tự động cập nhật phần mềm phòng chống mã độc, chế độ tự động rà quét mã độc khi sao chép, mở các tập tin hoặc trước khi kết nối các thiết bị lưu trữ dữ liệu di động với máy tính của CCVC, người lao động chế độ rà quét máy tính định kỳ hằng tuần. Ưu tiên sử dụng phần mềm có bản quyền (hệ điều hành, phần mềm phòng chống mã độc, phần mềm soạn thảo văn bản …). Các máy tính dành cho CCVC, người lao động tiếp nhận hồ sơ tại Bộ phận tiếp nhận và trả kết quả các cấp cần phải bảo đảm trang bị các phần mềm có bản quyền: hệ điều hành, phần mềm soạn văn bản và phần mềm phòng chống mã độc (kết nối về Trung tâm giám sát an toàn không gian mạng quốc gia).

b) Chỉ cài đặt phần mềm hợp lệ (phần mềm có bản quyền thương mại, phần mềm nội bộ được đầu tư hoặc phần mềm mã nguồn mở có nguồn gốc rõ ràng) và thuộc danh mục phần mềm được phép sử dụng do cơ quan, đơn vị có thẩm quyền ban hành (nếu có) hoặc được sự đồng ý bằng văn bản của người đứng đầu cơ quan, đơn vị; không tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận phụ trách, chuyên trách về ATTT mạng; thường xuyên cập nhật phần mềm và hệ điều hành. Tuyệt đối không tự ý lắp đặt thêm thiết bị; không sử dụng phần mềm bên thứ ba hoặc công cụ tự nghiên cứu, phát triển riêng nhưng chưa được cơ quan chuyên trách về ATTT mạng kiểm tra, đánh giá an ninh, ATTT để tra cứu, khai thác Cơ sở dữ liệu quốc gia về dân cư.

c) Chỉ truy cập vào các trang, cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn, nhiệm vụ của CCVC, người lao động; sử dụng những trình duyệt an toàn; không truy nhập, mở các trang tin, thư điện tử không rõ nguồn gốc; không sử dụng tính năng lưu mật khẩu tự động hoặc đăng nhập tự động. Các hệ thống phải được đăng xuất khi không sử dụng; thường xuyên xóa các biểu mẫu, mật khẩu, bộ nhớ đệm và phiên đăng nhập được lưu trong trình duyệt trên máy tính.

d) Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính (máy chạy chậm bất thường, cảnh bảo từ phần mềm phòng, chống phần mềm độc hại, mất dữ liệu,…), phải tắt máy và báo trực tiếp cho bộ phận phụ trách, chuyên trách về ATTT mạng để được xử lý kịp thời.

đ) Thực hiện thao tác khóa máy tính (sử dụng tính năng có sẵn trên máy tính) khi rời khỏi nơi đặt máy tính; phải tắt máy tính khi rời khỏi cơ quan.

e) Báo cáo và phải được thủ trưởng cơ quan, đơn vị đồng ý, cho phép trước khi mang máy tính, thiết bị CNTT có kết nối mạng thuộc sở hữu riêng đến nơi làm việc và kết nối với mạng nội bộ để thực hiện xử lý công việc. Trong trường hợp này, cá nhân phải tuân thủ đầy đủ các quy định tại các điểm a, b, c, d, đ khoản này và chịu sự giám sát của bộ phận phụ trách, chuyên trách về ATTT mạng của cơ quan, đơn vị.

g) Trường hợp mang máy tính, thiết bị CNTT của cơ quan ra khỏi cơ quan phải báo cáo và được sự đồng ý cả thủ trưởng cơ quan, đơn vị. Trong trường hợp này, cá nhân tuân thủ đầy đủ các quy định tại các điểm a, b, c, d, đ khoản này và có trách nhiệm theo khoản 3 Điều 19 của Quy chế này.

2. Khi thực hiện mua sắm trang thiết bị, máy tính liên quan đến bí mật nhà nước, phải được kiểm định ATTT của cơ quan có thẩm quyền trước khi đưa vào sử dụng.

3. Khuyến khích các cơ quan, đơn vị đầu tư, mua sắm thiết bị CNTT sản xuất trong nước. Không mua sắm thiết bị CNTT thuộc danh mục sản phẩm, hàng hóa có khả năng gây mất an toàn thuộc trách nhiệm quản lý của Bộ Thông tin và Truyền thông quy định.

4. Quản lý hệ thống mạng không dây

a) Khi thiết lập mạng không dây để kết nối với mạng cục bộ thông qua các điểm truy nhập (Access Point - AP), cơ quan, đơn vị vận hành phải thiết lập các tham số: Tên, nhận dạng dịch vụ (Service Set Identifier - SSID), mật khẩu mạnh, cấp phép truy nhập đối với địa chỉ vật lý (MAC Address), mã hóa dữ liệu theo cơ chế bảo mật WPA2 hoặc WPA3.

b) Mật khẩu đăng nhập phải được thiết lập có độ phức tạp cao, định kỳ 6 tháng thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

c) Khi cung cấp truy cập Internet qua mạng không dây cho người ngoài cơ quan, đơn vị sử dụng, cơ quan, đơn vị vận hành phải tạo thêm một SSID riêng, phân lớp, phân vùng mạng riêng, tách biệt mạng LAN nội bộ cơ quan, giới hạn băng thông và có mật khẩu truy cập phù hợp đối với đối tượng này. Trường hợp người ngoài cơ quan, đơn vị muốn sử dụng mạng không dây nội bộ cơ quan thì phải được thủ trưởng cơ quan, đơn vị đồng ý, cho phép.

Điều 12. Giám sát an toàn hệ thống thông tin

1. Chủ quản hệ thống thông tin phải triển khai hệ thống giám sát ATTT đáp ứng các yêu cầu tại Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin.

2. Sở Thông tin và Truyền thông có trách nhiệm tổ chức giám sát ATTT mạng đối với các hệ thống thông tin được đặt tại Trung tâm tích hợp dữ liệu tỉnh.

3. Đối với các hệ thống thông tin, phần mềm, ứng dụng, cơ sở dữ liệu không được đặt tại Trung tâm tích hợp dữ liệu tỉnh thì chủ quản hệ thống thông tin có trách nhiệm tự thực hiện hoặc yêu cầu doanh nghiệp cung cấp dịch vụ bảo đảm các yêu cầu giám sát an toàn hệ thống thông tin theo quy định của pháp luật.

4. Định kỳ hàng năm tổ chức đánh giá, kiểm tra đối với hệ thống thông tin nội bộ tại cơ quan, đơn vị. Thực hiện các biện pháp bảo trì cần thiết để bảo đảm khả năng xử lý và tính sẵn sàng của hệ thống thông tin.

5. Thủ trưởng cơ quan, đơn vị thành lập Tổ giám sát và xử lý sự cố ATTT mạng tại các cơ quan, đơn vị. Trường hợp không đủ điều kiện thành lập Tổ giám sát và xử lý sự cố ATTT mạng thì việc giám sát và xử lý sự cố ATTT mạng sẽ do bộ phận phụ trách về ATTT mạng, chuyển đổi số của cơ quan, đơn vị thực thiện.

Điều 13. Ứng cứu sự cố an toàn thông tin mạng

1. Nguyên tắc điều phối, ứng cứu sự cố theo quy định tại Điều 4 Thông tư số 20/2017/TT-BTTT ngày 12 tháng 9 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố ATTT mạng trên toàn quốc.

2. Phân nhóm sự cố ATTT

a) Sự cố do bị tấn công mạng: tấn công từ chối dịch vụ; tấn công giả mạo; tấn công sử dụng mã độc; truy cập trái phép, chiếm quyền điều khiển; tấn công thay đổi giao diện; tấn công mã hóa phần mềm, dữ liệu, thiết bị; phá hoại thông tin, dữ liệu, phần mềm; nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu; các hình thức tấn công mạng khác.

b) Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật.

c) Sự cố do lỗi của người quản trị, vận hành hệ thống.

d) Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn.

3. Phân loại mức độ nghiêm trọng sự cố

a) Thấp: sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan, đơn vị.

b) Trung bình: sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của cơ quan, đơn vị.

c) Cao: sự cố tác động đến khả năng vận hành của hệ thống thông tin, ảnh hưởng đến dữ liệu, thiết bị, gây ảnh hưởng đến hoạt động chung của cơ quan, đơn vị và hoạt động cung cấp dịch vụ công cho người dân, doanh nghiệp.

d) Nghiêm trọng: sự cố gây gián đoạn hoặc đình trệ hệ thống trong một khoảng thời gian ngắn, ảnh hưởng nghiêm trọng đến dữ liệu, thiết bị của hệ thống, gây thiệt hại nghiêm trọng cho cơ quan, đơn vị và người dân, doanh nghiệp.

4. Quy trình phối hợp ứng cứu sự cố

a) Bước 1: Nếu hệ thống có nguy cơ mất ATTT mạng thuộc thẩm quyền cơ quan, đơn vị trực tiếp quản lý thì thực hiện tiếp Bước 2. Nếu hệ thống có nguy cơ mất ATTT mạng thuộc Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Thông tin và Truyền thông quản lý (các hệ thống được triển khai tập trung tại Trung tâm tích hợp Dữ liệu tỉnh) thì thực hiện tiếp Bước 3.

b) Bước 2: Tiến hành xử lý sự cố theo quy chế nội bộ của cơ quan, đơn vị. Nếu sự cố được khắc phục thì lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố. Khi sự cố vượt quá khả năng xử lý của cơ quan, đơn vị, lập biên bản ghi nhận và thực hiện tiếp Bước 3.

c) Bước 3: Báo sự cố đến Sở Thông tin và Truyền thông theo mẫu số 03 ban hành kèm theo Thông tư số 20/2017/TT-BTTTT.

d) Bước 4: Phối hợp với Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Thông tin và Truyền thông và các cơ quan, đơn vị, tổ chức có liên quan để tiến hành khắc phục sự cố và thực hiện tiếp Bước 5.

đ) Bước 5: Lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố theo mẫu số 04 ban hành kèm theo Thông tư số 20/2017/TT-BTTTT. Lãnh đạo cơ quan, đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại, báo cáo bằng văn bản cho cơ quan cấp trên trực tiếp quản lý và Sở Thông tin và Truyền thông.

5. Trường hợp có sự cố ở mức độ cao, nghiêm trọng, khẩn cấp hoặc vượt quá khả năng khắc phục của cơ quan, đơn vị; lãnh đạo cơ quan, đơn vị phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và Sở Thông tin và Truyền thông để được hướng dẫn, hỗ trợ.

6. Đơn vị chuyên trách về ATTT (Sở Thông tin và Truyền thông) có trách nhiệm:

a) Xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố ATTT mạng, ứng phó sự cố ATTT mạng.

b) Xây dựng quy trình ứng cứu sự cố ATTT mạng theo quy định.

c) Phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố ATTT; yêu cầu bên cung cấp dịch vụ hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống.

d) Tổ chức diễn tập phương án xử lý sự cố ATTT.

Chương III
KIỂM TRA ĐÁNH GIÁ CÔNG TÁC BẢO ĐẢM ATTT MẠNG

Điều 14. Kế hoạch kiểm tra hàng năm

1. Sở Thông tin và Truyền thông chủ trì, phối hợp với Công an tỉnh và các đơn vị liên quan tiến hành kiểm tra công tác đảm bảo ATTT đối với các cơ quan, đơn vị trên địa bàn tỉnh theo Kế hoạch công tác hàng năm.

2. Tiến hành kiểm tra đột xuất các cơ quan, đơn vị khi có dấu hiệu vi phạm ATTT mạng đối với các hệ thống thông tin trên địa bàn tỉnh

Điều 15. Thẩm quyền, nội dung, hình thức, đối tượng kiểm tra, đánh giá hệ thống thông tin

1. Nội dung kiểm tra, đánh giá

a) Kiểm tra việc thực hiện theo các nội dung theo Quy chế này; việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ; kiểm tra

hiệu quả của các biện pháp, phương án bảo đảm, ứng phó, khắc phục sự cố ATTT mạng.

b) Đánh giá hiệu quả của biện pháp bảo đảm an toàn hệ thống thông tin; phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống.

c) Kiểm tra công tác giám sát ATTT và ứng phó khi xảy ra sự cố ATTT.

d) Kiểm tra, đánh giá các nội dung khác theo quy định của chủ quản hệ thống thông tin.

2. Hình thức kiểm tra, đánh giá

a) Kiểm tra, đánh giá định kỳ theo kế hoạch của chủ quản hệ thống thông tin và đơn vị chuyên trách về ATTT của tỉnh.

b) Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền.

3. Thẩm quyền yêu cầu kiểm tra, đánh giá

a) Đơn vị chuyên trách ATTT tại Trung ương.

b) Ủy ban nhân dân tỉnh hoặc Sở Thông tin và Truyền thông (đơn vị chuyên trách về ATTT trên địa bàn tỉnh).

c) Đơn vị chủ trì kiểm tra, đánh giá là đơn vị được cấp có thẩm quyền giao nhiệm vụ hoặc được lựa chọn để thực hiện nhiệm vụ kiểm tra, đánh giá.

4. Đối tượng kiểm tra, đánh giá là chủ quản hệ thống thông tin hoặc đơn vị vận hành hệ thống thông tin.

Chương IV

TRÁCH NHIỆM BẢO ĐẢM ATTT MẠNG VÀ TỔ CHỨC THỰC HIỆN

Điều 16. Trách nhiệm của Sở Thông tin và Truyền thông

1. Tham mưu giúp Ủy ban nhân dân tỉnh về công tác bảo đảm ATTT mạng trên địa bàn tỉnh và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong việc bảo đảm ATTT mạng cho Trung tâm tích hợp dữ liệu của tỉnh.

2. Thực hiện thủ tục xác định cấp độ ATTT và bảo đảm an toàn cho các hệ thống thông tin theo quy định của Luật ATTT mạng; Nghị định số 85/2016/NĐ-CP.

3. Chủ trì, phối hợp với Công an tỉnh và các cơ quan, đơn vị có liên quan tiến hành kiểm tra công tác bảo đảm ATTT mạng định kỳ hàng năm hoặc đột xuất khi có yêu cầu của cơ quan nhà nước có thẩm quyền.

4. Hàng năm, xây dựng và triển khai các Kế hoạch đào tạo, tập huấn về công tác bảo đảm ATTT mạng cho CCVC phụ trách về ATTT mạng của các cơ quan, đơn vị. Tổ chức diễn tập, diễn tập thực chiến ứng cứu sự cố ATTT mạng; tổ chức các hội

nghị, hội thảo chuyên đề và tuyên truyền về ATTT mạng trong công tác quản lý nhà nước trên địa bàn tỉnh.

5. Phối hợp với Công an tỉnh trong công tác phòng ngừa, phát hiện, ngăn chặn và xử lý các hành vi vi phạm pháp luật trên môi trường mạng, nhất là trên các cổng/trang thông tin điện tử, mạng xã hội theo thẩm quyền.

6. Là cơ quan đầu mối, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về ATTT mạng; tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về ATTT mạng trên địa bàn tỉnh.

7. Tham mưu, thành lập các Tổ, Nhóm chịu trách nhiệm quản lý ATTT theo cấp độ, theo phân cấp phê duyệt hồ sơ cấp độ về ATTT.

Điều 17. Trách nhiệm Công an tỉnh

1. Triển khai hoạt động bảo vệ dữ liệu cá nhân, bảo vệ quyền của chủ thể dữ liệu trước các hành vi vi phạm quy định của pháp luật về bảo vệ dữ liệu cá nhân trên địa bàn tỉnh.

2. Phối hợp Sở Thông tin và Truyền thông và các cơ quan có liên quan thực hiện kiểm tra, giải quyết khiếu nại, tố cáo, xử lý hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân theo quy định của pháp luật.

Điều 18. Trách nhiệm của các cơ quan, đơn vị

1. Chịu trách nhiệm trong công tác bảo đảm ATTT mạng của cơ quan, đơn vị mình theo Quy chế này và các quy định nhà nước về an toàn, an ninh thông tin khác.

2. Thực hiện xác định cấp độ ATTT và bảo đảm an toàn cho hệ thống thông tin của đơn vị quản lý theo quy định tại Luật ATTT mạng và Nghị định số 85/2016/NĐ-CP.

3. Phân công bộ phận hoặc nhân sự phụ trách về ATTT mạng bảo đảm ATTT mạng của cơ quan, đơn vị; chỉ đạo CCVC, người lao động nghiêm túc chấp hành các quy định về bảo đảm ATTT; tạo điều kiện để các CCVC phụ trách về ATTT mạng được học tập, nâng cao trình độ về ATTT; thường xuyên tổ chức quán triệt các quy định về ATTT trong cơ quan, đơn vị; xác định các yêu cầu, trách nhiệm bảo đảm ATTT đối với các vị trí cần tuyển dụng hoặc phân công.

4. Thường xuyên tổ chức, phổ biến các quy định về đảm bảo ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT cho tổ chức, cá nhân sử dụng hệ thống thông tin do cơ quan, đơn vị quản lý.

5. Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả.

6. Phối hợp chặt chẽ với Công an tỉnh, Sở Thông tin và Truyền thông và các cơ quan, đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm ATTT trên không gian mạng.

7 Hàng năm bố trí kinh phí cho việc ứng dụng CNTT nói chung và công tác bảo đảm ATTT mạng nói riêng trong nội bộ cơ quan, đơn vị mình; lập kế hoạch nâng cấp, bảo trì, sửa chữa, gia hạn bản quyền phần mềm... cho các hệ thống phần cứng, phần mềm nhằm thực hiện tốt công tác bảo mật, bảo đảm ATTT mạng đưa vào dự toán chi năm sau để triển khai thực hiện.

8. Các cơ quan, đơn vị cử đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố ATTT.

9. Đề xuất thành lập Tổ quản trị và vận hành kỹ thuật hệ thống thông tin theo cấp độ do cơ quan, đơn vị phụ trách, quản lý.

10. Thực hiện các báo cáo về ATTT mạng khi được Sở Thông tin và Truyền thông yêu cầu.

Điều 19. Trách nhiệm của cán bộ, công chức, người lao động trong các cơ quan, đơn vị

1. Trách nhiệm của nhân sự phụ trách về ATTT mạng tại cơ quan, đơn vị:

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về ATTT mạng. Chịu trách nhiệm về các hành vi làm mất ATTT mạng do không tuân thủ Quy chế này và các quy định của pháp luật có liên quan.

b) Tham mưu lãnh đạo cơ quan ban hành các quy chế, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm ATTT mạng.

c) Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố ATTT mạng.

d) Thường xuyên cập nhật nâng cao kiến thức, trình độ chuyên môn đáp ứng yêu cầu bảo đảm ATTT mạng của đơn vị.

2. Trách nhiệm của người sử dụng

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về ATTT mạng. Chịu trách nhiệm bảo đảm ATTT mạng trong phạm vi trách nhiệm và quyền hạn được giao.

b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng.

c) Khi phát hiện nguy cơ hoặc sự cố mất ATTT mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách ATTT mạng của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý.

d) Tham gia các chương trình đào tạo, hội nghị về ATTT mạng được cơ quan hoặc đơn vị chuyên môn tổ chức.

đ) CCVC được giao nhiệm vụ quản lý, vận hành truy cập, khai thác đối với các hệ thống thông tin thực hiện theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài; theo dõi và phát hiện các trường hợp truy cập hệ thống trái

phép hoặc thao tác vượt quá giới hạn, báo cáo cho cán bộ quản lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

Điều 20. Trách nhiệm của các tổ chức, cá nhân liên quan

Các tổ chức, cá nhân liên quan đến sử dụng, khai thác các hệ thống thông tin hoặc liên quan đến việc triển khai hoạt động ứng dụng CNTT, chuyển đổi số của các cơ quan nhà nước trên địa bàn tỉnh phải tuân thủ Quy chế này và các quy định hiện hành của pháp luật về an toàn, an ninh thông tin mạng.

Điều 21. Tổ chức thực hiện

1. Căn cứ Quy chế này, thủ trưởng các cơ quan, đơn vị trên địa bàn tỉnh và các đơn vị liên quan có trách nhiệm tổ chức triển khai thực hiện Quy chế này trong phạm vi quản lý của mình.

2. Trường hợp văn bản quy phạm pháp luật được viện dẫn tại Quy chế này được sửa đổi, bổ sung hoặc thay thế bằng văn bản quy phạm pháp luật khác thì thực hiện theo nội dung của văn bản quy phạm pháp luật sửa đổi, bổ sung hoặc thay thế đó.

3. Sở Thông tin và Truyền thông có trách nhiệm theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy chế, báo cáo Ủy ban nhân dân tỉnh theo định kỳ hằng năm hoặc đột xuất theo yêu cầu của cơ quan có thẩm quyền.

4. Trong quá trình thực hiện quy chế, nếu có vấn đề vướng mắc, phát sinh, các cơ quan, đơn vị phản ánh kịp thời về Ủy ban nhân dân tỉnh (thông qua Sở Thông tin và Truyền thông) để xem xét điều chỉnh, bổ sung./.