VĂN BẢN QUY PHẠM PHÁP LUẬT

ỦY BAN NHÂN DÂN TỈNH KHÁNH HÒA

ỦY BAN NHÂN DÂN **TỈNH KHÁNH HÒA**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 11/2026/QĐ-UBND	*Khánh Hòa, ngày 31 tháng 01 năm 2026*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an ninh mạng, an toàn thông tin trên địa bàn tỉnh Khánh Hòa

Căn cứ Luật Tổ chức Chính quyền địa phương số 72/2025/QH15;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật số 64/2025/QH15 đã được sửa đổi, bổ sung bởi Luật số 87/2025/QH15;

Căn cứ Luật Công nghệ thông tin số 67/2006/QH11;

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13;

Căn cứ Luật An ninh mạng số 24/2018/QH14;

Căn cứ Luật Bảo vệ bí mật nhà nước số 29/2018/QH14;

Căn cứ Luật Giao dịch điện tử số 20/2023/QH15;

Căn cứ Luật Dữ liệu số 60/2024/QH15;

Căn cứ Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15;

Căn cứ Nghị định số 150/2025/NĐ-CP ngày 12 tháng 6 năm 2025 của Chính phủ quy định tổ chức các cơ quan chuyên môn thuộc Ủy ban nhân dân cấp tỉnh và cấp xã;

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 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 147/2024/NĐ-CP ngày 09 tháng 11 năm 2024 của Chính phủ về quản lý, cung cấp và sử dụng dịch vụ Internet và thông tin trên không gian mạng;

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 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 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;

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 số 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 19/2023/TT-BTTTT ngày 25 tháng 12 năm 2023 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Quyết định số 08/2023/QĐ-TTg ngày 05 tháng 4 năm 2023 của Thủ tướng Chính phủ về Mạng truyền số liệu chuyên dùng phục vụ các cơ quan Đảng, Nhà nước;

Theo đề nghị của Giám đốc Công an tỉnh tại Tờ trình số 915/TTr-CAT(ANM) ngày 27 tháng 01 năm 2026;

Ủy ban nhân dân ban hành Quyết định ban hành Quy chế bảo đảm an ninh mạng, an toàn thông tin trên địa bàn tỉnh Khánh Hòa.

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an ninh mạng, an toàn thông tin trên địa bàn tỉnh Khánh Hòa; gồm 4 Chương, 33 Điều.

Điều 2. Hiệu lực thi hành

Quyết định này có hiệu lực kể từ ngày 31 tháng 01 năm 2026 và bãi bỏ các quy định trước đây của Ủy ban nhân dân tỉnh Khánh Hòa và Ủy ban nhân dân tỉnh Ninh Thuận trước sáp nhập, bao gồm:

a) Quyết định số 38/2015/QĐ-UBND ngày 24 tháng 12 năm 2015 của Ủy ban nhân dân tỉnh Khánh Hòa ban hành Quy định đảm bảo an toàn thông tin số trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Khánh Hòa.

b) Quyết định số 76/2024/QĐ-UBND ngày 24 tháng 9 năm 2024 của Ủy ban nhân dân tỉnh Ninh Thuận ban hành Quy chế về bảo đảm an ninh mạng, an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan Nhà nước trên địa bàn tỉnh Ninh Thuận.

Điều 3. Tổ chức thực hiện

Chánh Văn phòng Ủy ban nhân dân tỉnh; Giám đốc Công an tỉnh; Giám đốc các Sở; Thủ trưởng các ban ngành, đơn vị sự nghiệp công lập thuộc tỉnh; Chủ tịch Ủy ban nhân dân các xã, phường, đặc khu và tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

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

Nguyễn Thanh Hà

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

QUY CHẾ

Bảo đảm an ninh mạng, an toàn thông tin trên địa bàn tỉnh Khánh Hòa

(Ban hành kèm theo Quyết định số 11/2026/QĐ-UBND ngày 31 tháng 01 năm 2026 của Ủy ban nhân dân tỉnh Khánh Hòa)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh

Quy chế này quy định về bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin tỉnh Khánh Hòa.

2. Đối tượng áp dụng

a) Các sở, ban, ngành, Ủy ban nhân dân xã, phường, đặc khu, đơn vị sự nghiệp công lập, cán bộ, công chức, viên chức và tổ chức, cá nhân có liên quan đến việc quản lý, vận hành, khai thác hệ thống thông tin tỉnh Khánh Hòa (viết tắt là cơ quan, đơn vị).

b) Các doanh nghiệp cung cấp dịch vụ viễn thông, công nghệ thông tin, an toàn thông tin, an ninh mạng, Internet; các doanh nghiệp, tổ chức, cá nhân có tham gia vào các hoạt động ứng dụng công nghệ thông tin, chuyển đổi số, an toàn thông tin, an ninh mạng của các cơ quan, đơn vị thuộc điểm a khoản 2 Điều này.

Điều 2. Giải thích từ ngữ

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

1. An ninh mạng là việc bảo đảm 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.

2. An toàn thông tin mạng là sự bảo vệ thông tin số và các hệ thống thông tin

trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

3. Hệ thống thông tin là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng.

4. Hạ tầng kỹ thuật công nghệ thông tin là tập hợp thiết bị máy chủ, máy trạm, thiết bị tường lửa, thiết bị cân bằng tải, thiết bị lưu trữ, thiết bị mạng, thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, mạng nội bộ, mạng diện rộng, mạng truyền số liệu chuyên dùng.

5. Phần mềm độc hại (mã độc) được quy định tại khoản 11 Điều 3 Luật An toàn thông tin mạng.

6. Giám sát an toàn hệ thống thông tin được quy định tại khoản 1 Điều 24 Luật An toàn thông tin mạng.

7. Sự cố an toàn thông tin mạng được quy định tại khoản 7 Điều 3 Luật An toàn thông tin mạng.

8. Ứng cứu sự cố an toàn thông tin mạng được quy định tại khoản 2 Điều 2 Thông tư số 20/2017/TT-BTTTT.

9. Chủ quản hệ thống thông tin được quy định tại khoản 1 Điều 4 Thông tư số 12/2022/TT-BTTTT là Ủy ban nhân dân tỉnh.

10. Đơn vị chuyên trách về an toàn thông tin của tỉnh là Công an tỉnh.

11. Đơn vị vận hành hệ thống thông tin là các cơ quan, đơn vị trên địa bàn tỉnh được Ủy ban nhân dân tỉnh giao nhiệm vụ quản lý, vận hành hệ thống thông tin. Trong trường hợp thuê dịch vụ công nghệ thông tin thì doanh nghiệp, tổ chức cung cấp dịch vụ đóng vai trò đơn vị vận hành hệ thống thông tin.

Điều 3. Nguyên tắc bảo đảm an ninh mạng, an toàn thông tin

1. Bảo đảm an ninh mạng, an toàn thông tin đối với các hoạt động ứng dụng công nghệ thông tin, giao dịch điện tử, chuyển đổi số của tỉnh tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật An toàn thông tin mạng và Điều 4 Nghị định số 85/2016/NĐ-CP và các quy định pháp luật khác có liên quan.

2. Người đứng đầu cơ quan, đơn vị là người chịu trách nhiệm trực tiếp chỉ đạo công tác bảo đảm an ninh mạng, an toàn thông tin. Xác định rõ quyền hạn, trách nhiệm của các cấp phó; các tập thể và cá nhân trực tiếp liên quan đến công tác bảo đảm an ninh mạng, an toàn thông tin và an ninh mạng; bố trí nhân sự để sẵn sàng xử lý sự cố an ninh mạng, an toàn thông tin đối với các hệ thống thông tin do đơn vị mình quản lý.

3. Thông tin có bí mật nhà nước được thực hiện theo quy định của Luật Bảo vệ bí mật nhà nước và các quy định pháp luật về bảo vệ bí mật nhà nước có liên quan.

4. Xử lý sự cố an toàn thông tin phải phù hợp với trách nhiệm, quyền hạn và bảo đảm lợi ích hợp pháp của cơ quan, đơn vị, cá nhân liên quan và theo quy định của pháp luật.

Điều 4. Các hành vi bị cấm

1. Các hành vi bị nghiêm cấm về an toàn, an ninh thông tin mạng và giao dịch điện tử quy định tại Điều 7 Luật An toàn thông tin mạng, Điều 8 Luật An ninh mạng, Điều 5 Luật Bảo vệ bí mật nhà nước, Điều 6 Luật Giao dịch điện tử, Điều 9 Luật Viễn thông.

2. Hành vi khác bị nghiêm cấm theo quy định của pháp luật.

Chương II
QUY ĐỊNH BẢO ĐẢM AN NINH MẠNG, AN TOÀN THÔNG TIN

Điều 5. Yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ

1. 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. Nội dung yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ thực hiện theo quy định tại Điều 9 Thông tư số 12/2022/TT-BTTTT.

2. Đánh giá, phân loại cấp độ an toàn thông tin của hệ thống thông tin

a) 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.

b) Đơn vị vận hành hệ thống thông tin của các cơ quan, đơn vị trên địa bàn tỉnh thực hiện xác định cấp độ và lập hồ sơ đề xuất cấp độ bao gồm các tài liệu thuyết minh được quy định tại Điều 7, 8, 9, 10, 11, 15 Nghị định số 85/2016/NĐ-CP và Điều 8 Thông tư số 12/2022/TT-BTTTT gửi đơn vị chuyên trách về an toàn thông tin thẩm định, đề nghị cấp có thẩm quyền phê duyệt hồ sơ đề xuất cấp độ an toàn thông tin.

3. 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 của Thông tư số 24/2020/TT-BTTTT.

Điều 6. An ninh mạng, an toàn thông tin đối với thuê dịch vụ công nghệ thông tin

1. Trách nhiệm của cơ quan, đơn vị trước khi sử dụng dịch vụ công nghệ thông tin:

Thiết lập các yêu cầu về bảo đảm an toàn thông tin phù hợp với cấp độ an toàn hệ thống thông tin của đơn vị và hoạt động thuê dịch vụ công nghệ thông tin.

2. Trách nhiệm của cơ quan, đơn vị trong quá trình sử dụng dịch vụ công nghệ thông tin

a) 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 an toàn thông tin theo quy định tại Quy định này, Luật An toàn thông tin mạng, Luật An ninh mạng và các quy định khác có liên quan.

b) 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.

3. Trách nhiệm của cơ quan, đơn vị khi phát hiện bên cung cấp dịch vụ có dấu hiệu vi phạm quy định bảo đảm an toàn thông tin

a) Tạm dừng hoặc đình chỉ hoạt động của bên cung cấp dịch vụ tùy theo mức độ vi phạm.

b) Thông báo chính thức các hành vi vi phạm của bên cung cấp dịch vụ.

c) Thu hồi ngay lập tức quyền truy cập hệ thống thông tin đã cấp cho bên cung cấp dịch vụ.

d) 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.

4. Trách nhiệm của cơ quan, đơn vị khi kết thúc 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.

Điều 7. Giám sát an toàn hệ thống thông tin

1. Nguyên tắc, yêu cầu, phương thức về hoạt động giám sát an toàn hệ thống thông tin thực hiện theo quy định tại Điều 3, 4, 5 Thông tư số 31/2017/TT- BTTTT.

2. Chủ quản hệ thống thông tin chỉ đạo thực hiện giám sát đối với các hệ thống thông tin thuộc phạm vi quản lý.

3. Đơn vị chuyên trách về an toàn thông tin của tỉnh làm đầu mối giám sát, cảnh báo an ninh mạng, an toàn thông tin của tỉnh; tổ chức giám sát tập trung 24/7 và bảo đảm kết nối, chia sẻ kết quả giám sát về Trung tâm ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT).

4. Các cơ quan, đơn vị cử cá nhân hoặc bộ phận làm đầu mối giám sát, cung cấp, tiếp nhận thông tin cảnh báo kịp thời với đơn vị chuyên trách về an toàn thông tin của tỉnh, Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao của Công an tỉnh nhằm tăng cường công tác đảm bảo an ninh mạng, an toàn

thông tin và phòng, chống tội phạm sử dụng công nghệ cao. Đầu mối giám sát tại cơ quan, đơn vị chịu trách nhiệm bảo đảm điều kiện kết nối tại điểm giám sát và triển khai giám sát trong phạm vi hệ thống thông tin của cơ quan, đơn vị mình; duy trì đầu mối 24/7 và kênh liên lạc khẩn cấp; thời gian phản hồi ban đầu không quá 60 phút.

5. Đối với hệ thống thông tin quan trọng về an ninh quốc gia, thực hiện giám sát an ninh mạng theo Điều 14 Luật An ninh mạng.

Điều 8. Ứng cứu sự cố an toàn thông tin

1. Đơn vị chuyên trách ứng cứu khẩn cấp sự cố an ninh mạng, an toàn thông tin:

Đơn vị chuyên trách ứng cứu khẩn cấp sự cố an ninh mạng, an toàn thông tin của tỉnh là Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh.

2. Nguyên tắc ứng cứu xử lý sự cố

Nguyên tắc ứng cứu xử lý sự cố thực hiện theo quy định tại khoản 3 Điều 4, khoản 2 Điều 13 Luật An toàn thông tin mạng và Điều 4 Thông tư số 20/2017/TT-BTTTT.

3. Phân loại sự cố an ninh mạng, an toàn thông tin

a) Sự cố do bị tấn công mạng.

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

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

d) Sự cố do các thảm họa tự nhiên.

4. Phân loại mức độ 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.

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.

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 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, người dân, doanh nghiệp.

e) Đặc biệt nghiêm trọng: Sự cố làm tê liệt toàn bộ hoạt động của hệ thống, gây thiệt hại đặc biệt nghiêm trọng cho cơ quan, người dân, doanh nghiệp, đe dọa trật tự an toàn xã hội.

5. Quy trình ứng cứu sự cố thực hiện theo Điều 11 Thông tư số 20/2017/TT-BTTTT và các quy định tại Kế hoạch ứng phó sự cố an toàn, an ninh mạng hàng năm của Ủy ban nhân dân tỉnh.

6. Trường hợp sự cố ở mức độ tại điểm c, d, e khoản 4 Điều này hoặc vượt quá khả năng khắc phục của đơn vị, lãnh đạo cơ quan, đơn vị phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và đơn vị chuyên trách về an toàn thông tin của tỉnh để được hướng dẫn, hỗ trợ hoặc điều phối ứng cứu sự cố an ninh mạng, an toàn thông tin.

7. Quá trình xử lý sự cố phải được ghi chép và lưu trữ tại đơn vị; bảo toàn bằng chứng, chứng cứ phục vụ cho việc kiểm tra, xử lý, khắc phục và phòng ngừa sự cố. Trong trường hợp sự cố có liên quan đến các vi phạm pháp luật, đơn vị có trách nhiệm thu thập và cung cấp chứng cứ cho cơ quan có thẩm quyền theo quy định của pháp luật.

8. Đơn vị/bộ phận chuyên trách về an toàn thông tin có trách nhiệm

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

b) Xây dựng quy trình ứng cứu sự cố an ninh mạng, an toàn thông tin thông thường và nghiêm trọng 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 an toàn thông tin; yêu cầu bên cung cấp dịch vụ cung cấp đầy đủ quy trình xử lý sự cố đối với dịch vụ thực hiện.

d) Tổ chức diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của người đứng đầu cơ quan, đơn vị.

Điều 9. Kiểm tra, đánh giá an ninh mạng, an toàn thông tin

1. Đơn vị chuyên trách về an toàn thông tin của tỉnh tham mưu, tổ chức thực hiện kiểm tra, đánh giá đối với các hệ thống thông tin trên địa bàn tỉnh theo yêu cầu của Chủ quản hệ thống thông tin; có thẩm quyền yêu cầu kiểm tra, đánh giá đối với các hệ thống thông tin do mình phê duyệt hồ sơ đề xuất cấp độ.

2. Đơn vị chủ trì kiểm tra, đánh giá là đơn vị chuyên trách về an toàn thông tin của tỉnh hoặc đơn vị tư vấn được lựa chọn để thực hiện việc kiểm tra, đánh giá. Đối tượng kiểm tra, đánh giá là đơn vị vận hành hệ thống thông tin và các hệ thống thông tin có liên quan.

3. Trong quá trình vận hành hệ thống thông tin, đơn vị vận hành hệ thống thông tin có trách nhiệm định kỳ giá hiệu quả của các biện pháp bảo đảm an toàn thông tin theo quy định tại khoản 3 Điều 22 Nghị định số 85/2016/NĐ-CP.

4. Nội dung, tần suất kiểm tra đánh giá thực hiện theo Điều 11, 12 Thông tư số 12/2022/TT-BTTTT.

5. Việc kiểm tra, đánh giá an ninh mạng, an toàn thông tin đối với hệ thống từ cấp độ 3 trở lên phải do tổ chức chuyên môn được cơ quan có thẩm quyền cấp phép; cơ quan nhà nước có chức năng, nhiệm vụ phù hợp hoặc do tổ chức chuyên môn được cấp có thẩm quyền chỉ định thực hiện.

Điều 10. Quản lý rủi ro, lỗ hổng, điểm yếu an toàn thông tin

1. Các cơ quan, đơn vị phối hợp với đơn vị chuyên trách về an toàn thông tin của tỉnh tổ chức quản lý lỗ hổng, điểm yếu an ninh mạng, an toàn thông tin.

a) Lập danh sách toàn bộ thiết bị, phần mềm công nghệ thông tin đang sử dụng trong phạm vi quản lý: nhãn hiệu phần cứng, tên phần mềm và phiên bản (hệ điều hành, cơ sở dữ liệu, ứng dụng, các tiện ích khác).

b) Thiết lập, duy trì kênh tiếp nhận thông tin về lỗ hổng, điểm yếu an ninh mạng, an toàn thông tin từ các cơ quan, tổ chức có chức năng cảnh báo về an toàn thông tin mạng; các đơn vị cung cấp thiết bị, phần mềm công nghệ thông tin thuộc phạm vi điểm a khoản này.

c) Quản lý, giám sát việc cài đặt bản vá lỗ hổng, điểm yếu an ninh mạng, an

toàn thông tin. Sử dụng và cập nhật liên tục các công cụ dò quét lỗ hổng, điểm yếu an ninh mạng, an toàn thông tin để các công cụ này có thể phát hiện được các lỗ hổng bảo mật mới nhất; hoặc sử dụng kết quả kiểm tra, đánh giá an ninh mạng, an toàn thông tin để xác định các lỗ hổng, điểm yếu của hệ thống thông tin.

d) Triển khai cài đặt bản vá lỗ hổng, điểm yếu an ninh mạng, an toàn thông tin sau khi bản vá được phát hành; áp dụng các biện pháp bảo vệ tạm thời trong trường hợp bản vá bảo mật chưa được phát hành hoặc chưa đủ điều kiện để triển khai.

2. Các cơ quan, đơn vị phối hợp với đơn vị chuyên trách về an toàn thông tin, đơn vị vận hành hệ thống thông tin và cơ quan, tổ chức có liên quan triển khai quản lý rủi ro an ninh mạng, an toàn thông tin trên cơ sở quản lý lỗ hổng, điểm yếu an ninh mạng, an toàn thông tin theo quy định tại khoản 1 Điều này và theo hướng dẫn của Bộ Công an, Bộ Khoa học và Công nghệ.

3. Trên cơ sở báo cáo kết quả kiểm tra, đánh giá an ninh mạng, an toàn thông tin hoặc cảnh báo nguy cơ gây mất an ninh mạng, an toàn thông tin từ đơn vị chuyên trách về an toàn thông tin của tỉnh hoặc các cơ quan có thẩm quyền khác, chủ quản hệ thống thông tin có trách nhiệm tự khắc phục hoặc lựa chọn đơn vị đủ năng lực để triển khai các phương án khắc phục. Kết thúc xử lý, báo cáo kết quả thực hiện về đơn vị chuyên trách về an toàn thông tin của tỉnh để theo dõi, tổng hợp.

Điều 11. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

Hệ thống thông tin khi kết thúc vận hành, khai thác hoặc thanh lý, hủy bỏ phải tuân thủ các quy định của pháp luật về quản lý, sử dụng tài sản công và được các cấp có thẩm quyền cho phép dừng sử dụng. Thông tin, dữ liệu trên các hệ thống thông tin phải được sao lưu và chuyển sang các hệ thống khác (nếu còn giá trị sử dụng). Thực hiện các biện pháp xóa, hủy dữ liệu trước khi thanh lý, hủy tài sản theo đúng quy định của pháp luật.

Điều 12. Bảo đảm an toàn, an ninh thông tin trong quản lý tài sản công nghệ thông tin

1. Phân loại tài sản công nghệ thông tin

a) Tài sản phần cứng (vật lý): Là các máy móc, trang thiết bị phần cứng, phương tiện truyền thông và các trang thiết bị phục vụ cho hoạt động của hệ thống thông tin.

b) Tài sản phần mềm: Là các phần mềm hệ thống, phần mềm thương mại, phần mềm nội bộ, phần mềm ứng dụng, phần mềm quản trị cơ sở dữ liệu và công cụ phát triển phần mềm.

c) Tài sản thông tin: Là các thông tin, cơ sở dữ liệu, dữ liệu ở dạng số hóa.

2. Yêu cầu về quản lý tài sản công nghệ thông tin

a) Giao, gắn trách nhiệm cho cá nhân hoặc tập thể quản lý, sử dụng tài sản công nghệ thông tin.

b) Quy định các quy tắc sử dụng, giữ gìn bảo vệ tài sản công nghệ thông tin trong các trường hợp như: Mang ra khỏi cơ quan, trang thiết bị công nghệ thông tin liên quan đến dữ liệu bảo mật, thông tin cài đặt và cấu hình.

c) Tài sản công nghệ thông tin phải được đặt tên theo quy định. Việc đặt tên các thiết bị công nghệ thông tin trong toàn tỉnh cần bảo đảm thống nhất, dễ quản lý, dễ phân loại và hỗ trợ truy vết nhanh chóng trong các tình huống vận hành, kiểm tra, bảo trì, giám sát hoặc xử lý sự cố. Công an tỉnh phối hợp với Sở Khoa học và Công nghệ hướng dẫn các cơ quan, đơn vị đặt tên theo quy định; tên thiết bị phải phản ánh rõ vị trí quản lý, loại thiết bị, đơn vị chủ quản và số thứ tự định danh.

d) Tài sản phần cứng có lưu trữ dữ liệu quan trọng khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị phải phối hợp với bộ phận chuyên trách về công nghệ thông tin thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó bảo đảm không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, đơn vị phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên trang thiết bị đó.

e) Trang thiết bị công nghệ thông tin có bộ phận lưu trữ dữ liệu hoặc thiết bị lưu trữ dữ liệu khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài hoặc ngừng sử dụng phải tháo bộ phận lưu trữ khỏi thiết bị và để lại cơ quan, đơn vị hoặc xóa thông tin, 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.

f) Các đơn vị có trách nhiệm bảo dưỡng, bảo trì và hướng dẫn cách sử dụng, quản lý, vận hành hệ thống hạ tầng kỹ thuật của mình; chỉ định bộ phận thực hiện quản lý, vận hành và định kỳ kiểm tra, sửa chữa, bảo trì thiết bị (bao gồm thiết bị đang hoạt động và thiết bị dự phòng).

Điều 13. Bảo đảm an toàn vật lý và môi trường vận hành

1. Các khu vực bố trí hạ tầng hệ thống xử lý, lưu trữ thông tin, phương tiện xử lý thông tin, phương tiện bảo đảm an ninh mạng, an toàn thông tin phải được đặt ở vị trí an toàn, tại các phòng chuyên biệt bảo đảm tiêu chuẩn quy định và phải được thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập, biện pháp kiểm soát truy cập, kết nối vật lý phù hợp với từng khu vực, bảo đảm chỉ người có nhiệm vụ mới được vào và phải có nội quy riêng khi làm việc trong các khu vực này.

2. Trung tâm Dữ liệu tỉnh là khu vực hạn chế tiếp cận, chỉ những cá nhân có quyền, nhiệm vụ theo quy định và được sự cho phép của cơ quan chủ quản là Ủy ban nhân dân tỉnh hoặc cơ quan quản lý, vận hành là Sở Khoa học và công nghệ mới được vào Trung tâm Dữ liệu. Việc vào, ra Trung tâm Dữ liệu tỉnh phải thực hiện theo nội quy quy định, được hệ thống kiểm soát vào ra (quẹt thẻ, vân tay, nhận dạng sinh trắc học…), lưu hồ sơ để truy vết khi có yêu cầu.

3. Các khu vực quy định tại khoản 1, 2 Điều này phải có biện pháp đảm bảo nguồn điện và dự phòng điện, phòng chống cháy nổ, ngập lụt, động đất, chống sét, tác động của môi trường và các thảm họa khác do thiên nhiên và con người gây ra.

4. Các đường truyền dữ liệu, đường truyền Internet và hệ thống dây dẫn các hệ thống mạng diện rộng (WAN), hệ thống mạng nội bộ (LAN) phải được lắp đặt trong ống, máng che đậy kín, hạn chế khả năng tiếp cận trái phép. Ngắt các cổng kết nối không sử dụng, đặc biệt là ở khu vực làm việc chung của các cơ quan, đơn vị.

5. Thiết lập cơ chế dự phòng đối với các thiết bị hạ tầng kỹ thuật quan trọng; có kế hoạch kiểm tra, bảo dưỡng định kỳ và duy trì thông số kỹ thuật các thiết bị này hoặc có phương án sửa chữa, thay thế đáp ứng yêu cầu về tính khả dụng.

6. Cơ quan, đơn vị có trách nhiệm xây dựng quy trình bảo dưỡng, bảo trì và hướng dẫn cách sử dụng, quản lý, vận hành hệ thống hạ tầng kỹ thuật của mình;

chỉ định bộ phận chuyên trách về an ninh mạng, an toàn thông tin thực hiện quản lý, vận hành và định kỳ kiểm tra, sửa chữa, bảo trì thiết bị (bao gồm thiết bị đang hoạt động và thiết bị dự phòng).

Điều 14. Quản lý an toàn hạ tầng mạng

1. An toàn cho mạng nội bộ (LAN)

a) Phải sử dụng thiết bị tường lửa chuyên dụng hoặc phần mềm tường lửa để ngăn chặn và phát hiện xâm nhập trái phép vào mạng nội bộ của cơ quan khi kết nối với hệ thống bên ngoài.

b) Khi kết nối từ xa vào mạng nội bộ, phải sử dụng giao thức mạng có mã hóa thông tin và thiết lập mật khẩu đủ mạnh theo quy định.

c) Mạng LAN phải được phân chia lớp bằng VLAN hoặc phân chia vật lý theo vùng bảo mật và chức năng, tối thiểu gồm:

(i) Vùng máy chủ/trung tâm dữ liệu;

(ii) Vùng máy trạm người dùng;

(iii) Vùng thiết bị chuyên dụng (IoT, thiết bị giám sát, camera…);

(iv) Vùng quản trị/thiết bị mạng;

(v) Vùng mạng trung gian đối với dịch vụ công bố ra Internet (nếu có).

d) Lưu lượng giữa các lớp/VLAN chỉ được phép đi qua thiết bị lớp 3 hoặc tường lửa; áp dụng nguyên tắc mặc định chặn, cho phép theo quy tắc; giới hạn quyền truy cập theo nhu cầu tối thiểu. Trên thiết bị chuyển mạch/định tuyến phải triển khai danh sách kiểm soát truy cập để kiểm soát truy cập giữa các VLAN và ghi nhật ký đầy đủ các kết nối liên VLAN theo quy định. Nghiêm cấm cấu hình định tuyến chéo trực tiếp giữa các VLAN trên thiết bị chuyển mạch khi không áp dụng cơ chế kiểm soát, giám sát và ghi nhật ký. Việc tạo, sửa đổi, hủy VLAN và điều chỉnh danh sách kiểm soát truy cập phải được quản lý tập trung, có phê duyệt theo thẩm quyền và lưu vết hồ sơ phục vụ kiểm tra, giám sát.

2. Mạng không dây để kết nối với mạng nội bộ phải thiết lập mật khẩu mạnh, mã hóa dữ liệu theo cơ chế bảo mật WPA2 hoặc WPA3. Mật khẩu truy cập phải được thay đổi định kỳ 03 tháng/lần.

3. Hệ điều hành, phần mềm tích hợp trên các thiết bị mạng phải có bản quyền và thường xuyên được cập nhật các bản vá lỗi theo khuyến nghị của nhà sản xuất.

4. Phải lưu nhật ký khi thay đổi cấu hình kỹ thuật của các thiết bị mạng.

Điều 15. Quản lý an toàn máy chủ và ứng dụng

1. Quản lý, vận hành hoạt động bình thường hệ thống máy chủ và dịch vụ

a) Máy chủ phải được cài đặt hệ điều hành có bản quyền, sử dụng phần mềm phòng chống mã độc, giám sát thiết bị đầu cuối, phòng chống thất thoát dữ liệu tập trung; phần mềm phải được cập nhật thường xuyên và có tính năng, giải pháp kỹ thuật bảo đảm an toàn an ninh mạng đáp ứng yêu cầu theo các quy định hiện hành của cơ quan chuyên trách về an toàn an ninh mạng.

b) Cấu hình phần cứng của máy chủ phải bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn.

c) Thiết lập chế độ tự động cập nhật hoặc thường xuyên cập nhật các bản vá hệ điều hành, phần mềm, ứng dụng và hệ quản trị cơ sở dữ liệu được cài đặt trên máy chủ, phải thiết lập mật khẩu chế độ tự động bảo vệ màn hình ngay sau khi không sử dụng đối với tất cả máy chủ.

d) Thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng.

e) Thường xuyên kiểm tra cấu hình, các tệp tin nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có.

f) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.

g) Bảo đảm các kết nối mạng trên máy chủ hoạt động liên tục, ổn định và an toàn. Cấu hình, kiểm soát các kết nối, các cổng dịch vụ từ bên trong đi ra, bên ngoài đi vào hệ thống.

h) Thường xuyên thực hiện rà soát, xây dựng phương án, kế hoạch thực hiện thay thế máy chủ, trang thiết bị mạng, phần mềm ứng dụng đã cũ, không bảo đảm hiệu quả, chất lượng vận hành.

2. Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống trước khi đưa vào sử dụng, vận hành, khai thác

a) Xây dựng, áp dụng quy trình cấu hình tối ưu, tăng cường bảo mật cho các máy chủ.

b) Máy chủ phải được rà soát, cấu hình tối ưu, tăng cường bảo mật trước khi đưa hệ thống vào vận hành khai thác.

3. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố

a) Triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: Tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu, thông tin nghiệp vụ.

b) Phải thực hiện lưu trữ thay đổi cấu hình kỹ thuật của máy chủ, hệ điều hành, phần mềm.

4. Nghiêm cấm sử dụng các tài nguyên tính toán (máy chủ, máy trạm) để thực hiện các hành vi vi phạm pháp luật, tấn công mạng hoặc các hoạt động bất hợp pháp khác.

Điều 16. Bảo đảm an ninh mạng, an toàn thông tin khi sử dụng máy tính và thiết bị ngoại vi

1. Máy tính và thiết bị ngoại vi của đơn vị phải được cài đặt hệ điều hành, phần mềm soạn thảo văn bản, phần mềm chuyên dụng để xử lý công việc và tuân thủ các quy định sau:

a) Chỉ cài đặt phần mềm hợp lệ (phần mềm có bản quyền thương mại, phần mềm nội bộ hoặc phần mềm mã nguồn mở được đầu tư (hoặc thuê dịch vụ) có nguồn gốc rõ ràng) và thuộc danh mục phần mềm được phép sử dụng do đơn vị có thẩm quyền của Ủy ban nhân dân tỉnh ban hành (nếu có); không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận chuyên trách về công nghệ thông tin; thường xuyên cập nhật phần mềm và hệ điều hành.

b) Cài đặt phần mềm xử lý phần mềm độc hại và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; thực hiện kiểm tra, rà quét phần mềm độc hại 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 mình.

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

d) Chỉ truy nhập 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 của mình; 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.

e) Có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác. Đặt mật khẩu với độ an toàn cao (tối thiểu 8 ký tự bao gồm: có chữ thường, có chữ in hoa, có số và ký tự đặc biệt như @, #, !,...) và thay đổi mật khẩu tối thiểu 6 tháng/lần; các tài khoản đăng nhập các hệ thống phải được đăng xuất khi không sử dụng; thường xuyên xóa bộ nhớ cache và cookie trong trình duyệt trên máy tính.

f) Thực hiện thao tác khóa máy tính (sử dụng tính năng có sẵn trên máy tính) khi rời khỏi nơi đặt máy tính; tắt máy tính khi rời khỏi đơn vị.

2. Trước khi mang máy tính, thiết bị công nghệ thông tin 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 phải báo cáo và phải được lãnh đạo đơn vị đồng ý, cho phép. Trong trường hợp này, cá nhân phải tuân thủ đầy đủ các quy định tại các điểm a, b, c, d, đ, e khoản 1 Điều này và chịu sự giám sát của bộ phận chuyên trách về công nghệ thông tin của đơn vị.

3. Đối với thiết bị soạn thảo, lưu trữ bí mật nhà nước:

a) Các đơn vị phải bố trí ít nhất một máy tính độc lập, máy in (photocopy) không kết nối và không có lịch sử 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 để soạn thảo, lưu trữ các văn bản có nội dung bí mật nhà nước.

b) Công chức, viên chức, nhân viên được giao nhiệm vụ trong quá trình xử lý

công việc, soạn thảo văn bản có nội dung bí mật nhà nước chỉ sử dụng máy tính, thiết bị theo quy định tại điểm a của mục này; việc lưu trữ phải được thực hiện ở các thiết bị riêng biệt, bảo đảm các yêu cầu của pháp luật về bảo vệ bí mật nhà nước và cơ yếu.

Điều 17. Bảo đảm an toàn thông tin Trung tâm Dữ liệu tỉnh

1. Đơn vị vận hành Trung tâm Dữ liệu là đơn vị chuyên trách về an toàn thông tin Trung tâm Dữ liệu; chịu trách nhiệm xây dựng, thực thi các quy định về an toàn bảo mật thông tin mạng, quản lý, khai thác và vận hành Trung tâm Dữ liệu.

2. Đơn vị vận hành Trung tâm Dữ liệu tỉnh có trách nhiệm thực hiện phân loại, đánh giá và xác định cấp độ an toàn hệ thống thông tin theo quy định hiện hành, tối thiểu phải được bảo đảm an toàn thông tin ở mức độ 3 và áp dụng các biện pháp kỹ thuật, mô hình tổ chức phù hợp với cấp độ đã được phê duyệt, phối hợp với các cơ quan, tổ chức có thẩm quyền về quản lý an ninh mạng, an toàn thông tin, công tác hỗ trợ điều phối xử lý sự cố an ninh mạng, an toàn thông tin, tham gia hoạt động đảm bảo an ninh mạng, an toàn thông tin. Tùy theo mức độ sự cố, phối hợp với các đơn vị có liên quan thực hiện hướng dẫn xử lý, ứng cứu sự cố an ninh mạng, an toàn thông tin cho các hệ thống thông tin dùng chung của tỉnh.

3. Cơ quan, đơn vị có hệ thống thông tin được cài đặt, duy trì vận hành tại Trung tâm Dữ liệu có trách nhiệm bảo đảm an toàn thông tin cho máy chủ, ứng dụng, các trang thiết bị công nghệ thông tin hoặc các thành phần đặc biệt khác phục vụ hệ thống thông tin của cơ quan, đơn vị mình. Chủ động phối hợp với đơn vị dịch vụ xây dựng phát triển hệ thống thông tin triển khai các biện pháp bảo đảm an ninh mạng, an toàn thông tin và theo yêu cầu của đơn vị vận hành Trung tâm Dữ liệu, thực hiện nghiêm các văn bản, tài liệu hướng dẫn về việc quản lý tài khoản người dùng sử dụng, khai thác hệ thống do Trung tâm Dữ liệu ban hành.

4. Các cơ quan, đơn vị thực hiện tích hợp, kết nối, sử dụng hạ tầng, dịch vụ của Trung tâm Dữ liệu chịu trách nhiệm nếu để tin tặc chiếm quyền kiểm soát máy vi tính (của người dùng cuối) và truy cập trái phép vào Trung tâm Dữ liệu của tỉnh, tuân thủ nghiêm các quy định tại Quy chế quản lý, vận hành, sử dụng Trung tâm

dữ liệu và mạng diện rộng của tỉnh Khánh Hòa ban hành kèm theo Quyết định số 1454/QĐ-UBND ngày 04 tháng 10 năm 2025 của Ủy ban nhân dân tỉnh.

Điều 18. Bảo đảm an toàn thông tin Trung tâm Phục vụ hành chính công

1. Trung tâm Phục vụ hành chính công tỉnh/cấp xã (sau đây gọi là Trung tâm) có trách nhiệm tổ chức thực hiện đầy đủ các biện pháp bảo đảm an ninh mạng, an toàn thông tin đối với toàn bộ hạ tầng công nghệ thông tin, hệ thống phần mềm, dữ liệu do Trung tâm quản lý, vận hành.

2. Giám đốc Trung tâm chịu trách nhiệm tổ chức triển khai và chỉ đạo toàn diện công tác bảo đảm an toàn thông tin tại đơn vị; phân công bộ phận hoặc cá nhân chuyên trách (kiêm nhiệm) về an toàn thông tin để thực hiện nhiệm vụ tham mưu, kiểm tra, giám sát, cảnh báo và chủ động phối hợp với các cơ quan, đơn vị chuyên trách về bảo đảm an toàn an ninh mạng thực hiện ứng cứu sự cố an toàn thông tin (nếu xảy ra).

3. Trung tâm có trách nhiệm thực hiện phân loại, đánh giá và xác định cấp độ an toàn hệ thống thông tin theo quy định hiện hành và áp dụng các biện pháp kỹ thuật, biện pháp quản lý phù hợp với cấp độ đã được phê duyệt.

4. Trung tâm tổ chức thực hiện đầy đủ các biện pháp kỹ thuật cần thiết nhằm bảo đảm an toàn thông tin, bao gồm: Phân vùng mạng cụ thể đối với các hệ thống thông tin thành phần; sử dụng tường lửa vật lý với các giải pháp bản quyền tích hợp kèm theo đúng tiêu chuẩn quy định; không lưu trữ mật khẩu trên trình duyệt; chỉ sử dụng hệ điều hành, phần mềm có bản quyền; sử dụng trang thiết bị công nghệ thông tin cấu hình tiêu chuẩn theo hướng dẫn của cơ quan chuyên môn; không sử dụng chung tài khoản để giải quyết thủ tục hành chính; không cài đặt, sử dụng phần mềm điều khiển từ xa hoặc các ứng dụng không phục vụ công việc.

5. Trung tâm xây dựng và triển khai quy trình quản lý sự cố an toàn thông tin, bảo đảm khả năng phát hiện, khoanh vùng, xử lý, khôi phục và báo cáo sự cố kịp thời. Trường hợp xảy ra sự cố nghiêm trọng, Trung tâm có trách nhiệm thông báo nhanh và bằng văn bản cho Công an tỉnh trong thời hạn không quá 12 giờ kể từ khi phát hiện.

6. Trung tâm có trách nhiệm tổ chức tự kiểm tra công tác bảo đảm an toàn thông tin định kỳ 06 tháng/lần; phối hợp với các cơ quan có thẩm quyền thực hiện kiểm tra, đánh giá an ninh an toàn độc lập tối thiểu 01 năm/lần; lưu trữ đầy đủ hồ sơ, biên bản kiểm tra, báo cáo sự cố trong thời hạn tối thiểu 05 năm để phục vụ công tác thanh tra, kiểm tra.

7. Trung tâm tổ chức đào tạo, bồi dưỡng kiến thức về an ninh mạng, an toàn thông tin cho toàn thể cán bộ, công chức, viên chức và người lao động ít nhất 01 lần/năm; đồng thời thực hiện tuyên truyền, phổ biến cảnh báo an toàn thông tin qua hệ thống nội bộ hoặc các hình thức phù hợp khác.

Điều 19. Bảo đảm an toàn dữ liệu

1. Quản lý tài khoản truy cập

a) Khi cấp tài khoản lần đầu cho người dùng, đơn vị vận hành hệ thống thông tin phải thông báo cho người dùng. Người dùng có trách nhiệm thay đổi mật khẩu sau khi đăng nhập thành công lần đầu. Chậm nhất là 03 ngày, các tài khoản không tuân thủ việc thay đổi mật khẩu phải được tự động vô hiệu hóa.

b) Các hệ thống thông tin phải thiết lập giới hạn số lần đăng nhập không hợp lệ tối đa không quá 05 lần; tự động kết thúc phiên làm việc nếu quá 30 phút người dùng không tương tác với hệ thống.

c) Khi cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu, đơn vị quản lý cá nhân đó phải thông báo cho đơn vị vận hành hệ thống thông tin để điều chỉnh, thu hồi hoặc hủy bỏ tài khoản.

d) Tài khoản quản trị hệ thống (mạng, hệ điều hành, thiết bị kết nối mạng, phần mềm, ứng dụng, cơ sở dữ liệu) phải tách biệt với tài khoản truy cập của người dùng thông thường. Được giao đích danh cá nhân đảm nhiệm vai trò quản trị hệ thống quản lý.

e) Tài khoản quản trị, tài khoản người dùng phải được rà soát hàng năm, đảm bảo các tài khoản và quyền truy cập hệ thống được cấp phát theo đúng chức năng, nhiệm vụ, quyền hạn của cán bộ, công chức. Các tài khoản không sử dụng trong thời gian 03 tháng phải bị khóa hoặc xóa bỏ (sau khi trao đổi, xác nhận với cơ quan, đơn vị sử dụng).

2. Cơ quan, đơn vị phải thực hiện bảo vệ thông tin, dữ liệu liên quan đến hoạt động công vụ, thông tin có nội dung quan trọng, nhạy cảm hoặc không phải là thông tin công khai bằng các biện pháp như: Thiết lập phương án bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu; mã hóa thông tin, dữ liệu khi lưu trữ trên hệ thống/thiết bị lưu trữ dữ liệu di động; sử dụng chữ ký số để xác thực và bảo mật thông tin, dữ liệu; xây dựng quy trình quản lý và phân công cán bộ quản lý.

3. Không soạn thảo, lưu giữ, truyền đưa tài liệu chứa bí mật nhà nước trên máy vi tính, các thiết bị khác đã kết nối hoặc đang kết nối với mạng Internet, mạng máy vi tính, mạng viễn thông, trừ trường hợp lưu giữ bí mật nhà nước theo quy định của pháp luật về cơ yếu.

4. Các cơ quan, đơn vị phải thường xuyên kiểm tra, giám sát các hoạt động chia sẻ, gửi, nhận thông tin, tài liệu, dữ liệu điện tử trong hoạt động nội bộ trên môi trường mạng; khuyến cáo việc chia sẻ, gửi, nhận thông tin trên môi trường mạng cần phải sử dụng mật khẩu mạnh để bảo vệ an toàn thông tin.

5. Giao dịch trực tuyến phải được truyền tải đầy đủ thông tin, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép; sử dụng các cơ chế xác thực đủ mạnh theo quy định, dùng chữ ký số khi tham gia giao dịch và sử dụng các giao thức truyền thông an toàn.

6. Sao lưu và khôi phục: thực hiện chiến lược sao lưu 3-2-1-1-0 (trong đó có ít nhất một bản sao bất biến/air-gap); kiểm thử khôi phục dữ liệu định kỳ tối thiểu 02 lần/năm; quy định mục tiêu thời gian khôi phục hệ thống sau sự cố/mục tiêu điểm khôi phục dữ liệu cho từng hệ thống.

7. Dữ liệu cá nhân được thực hiện theo Nghị định số 13/2023/NĐ-CP; Luật Bảo vệ dữ liệu cá nhân và các văn bản hướng dẫn thi hành.

Điều 20. Bảo đảm an toàn thiết bị và người dùng đầu cuối

1. Trên máy tính công vụ phải thực hiện đầy đủ các biện pháp bảo mật phần mềm (cập nhật hệ điều hành, cài đặt phần mềm phòng chống mã độc, giám sát thiết bị đầu cuối, phòng chống thất thoát dữ liệu…), thiết lập mật khẩu truy cập bảo vệ

màn hình khi không sử dụng; cài đặt, sử dụng phần mềm hợp lệ (phần mềm có bản quyền, 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 có thẩm quyền ban hành (nếu có); không truy cập các trang tin nghi ngờ chứa mã độc hoặc các nội dung không phù hợp; thiết lập chế độ rà quét mã độc máy tính định kỳ.

2. Các cơ quan, đơn vị đầu tư, thuê, mua sắm thiết bị đảm bảo an toàn thông tin ưu tiên các sản phẩm, dịch vụ sản xuất trong nước theo quy định tại Thông tư số 40/2020/TT-BTTTT. Cấu hình thiết bị phải bảo đảm tiêu chuẩn, yêu cầu theo hướng dẫn của các bộ ngành Trung ương, cơ quan chuyên môn liên quan (nếu có) và bảo đảm việc vận hành, khai thác, sử dụng và triển khai đầy đủ các giải pháp bảo đảm an ninh mạng, an toàn thông tin.

3. Kết nối máy vi tính/thiết bị đầu cuối của người sử dụng vào hệ thống

a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của cơ quan, tổ chức.

b) Khi cài đặt, kết nối máy vi tính/thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của bộ phận chuyên trách về an toàn thông tin.

c) Đối với hệ thống thông tin từ cấp độ 3 trở lên, máy vi tính/thiết bị đầu cuối phải được cơ quan, đơn vị chuyên trách công nghệ thông tin kiểm tra, rà soát xử lý điểm yếu, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống.

4. Trong quá trình sử dụng thiết bị đầu cuối

a) Người sử dụng chỉ được phân quyền tối thiểu để sử dụng máy vi tính được trang cấp, không được phép tự ý cài đặt các phần mềm, sao chép tài liệu, dữ liệu điện tử hoặc kết nối các thiết bị ngoại vi chưa rõ nguồn gốc xuất xứ vào máy vi tính công vụ. Việc cài đặt và phân quyền do cán bộ chuyên trách về công nghệ thông tin của đơn vị thực hiện hoặc giám sát thực hiện.

b) Nghiêm túc chấp hành các quy định, quy trình nội bộ và các quy định khác của pháp luật về an ninh mạng, an toàn thông tin, bảo vệ bí mật nhà nước và dữ liệu cá nhân. Chịu trách nhiệm bảo đảm an toàn an ninh mạng trong phạm vi trách nhiệm và quyền hạn được giao.

c) Có trách nhiệm tự quản lý, bảo quản trang, thiết bị, máy vi tính, tài khoản, ứng dụng mà mình được giao để sử dụng.

d) Khi phát hiện nguy cơ hoặc sự cố mất an ninh mạng, an toàn thông tin phải báo cáo ngay với cấp trên trực tiếp và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý.

Điều 21. Bảo đảm nguồn nhân lực an ninh mạng, an toàn thông tin

1. Công chức, viên chức, người lao động được tuyển dụng hoặc sắp xếp, giao nhiệm vụ về an ninh mạng, an toàn thông tin phải có trình độ, chuyên ngành phù hợp yêu cầu đối với các vị trí việc làm về công nghệ thông tin, an ninh mạng, an toàn thông tin theo hướng dẫn của cơ quan nhà nước có thẩm quyền.

2. Cán bộ chuyên trách về công nghệ thông tin trong các cơ quan, đơn vị được tạo điều kiện trang bị các thiết bị công nghệ thông tin, phương tiện kỹ thuật làm việc phù hợp với chuyên môn; tham dự đầy đủ các khóa đào tạo, tập huấn và bồi dưỡng kiến thức, kỹ năng, nghiệp vụ cho cán bộ chuyên trách về an ninh mạng, an toàn thông tin.

3. Các cơ quan, đơn vị xác định nhu cầu về đào tạo nguồn nhân lực bảo đảm an toàn thông tin tại cơ quan, đơn vị mình gửi Công an tỉnh tổng hợp, trình Ủy ban nhân dân tỉnh phê duyệt kế hoạch giai đoạn, kế hoạch hàng năm về đào tạo, bồi dưỡng nghiệp vụ bảo đảm an ninh mạng, an toàn thông tin cho cán bộ, công chức, viên chức và người lao động của tỉnh và thực hiện tổ chức đào tạo theo kế hoạch đã phê duyệt.

4. Các cơ quan, đơn vị hàng năm phải tổ chức ít nhất 01 hoạt động tuyên truyền, phổ biến nâng cao nhận thức về chuyển đổi số, bảo đảm an ninh mạng, an toàn thông tin và an ninh mạng đến toàn thể cán bộ, công chức, viên chức và người lao động tại cơ quan, đơn vị mình.

Chương III
TRÁCH NHIỆM BẢO ĐẢM AN NINH MẠNG, AN TOÀN THÔNG TIN

Điều 22. Trách nhiệm của Công an tỉnh

1. Tham mưu giúp Ủy ban nhân dân tỉnh thực hiện thống nhất quản lý nhà nước về bảo đảm an ninh mạng, an toàn thông tin và chịu trách nhiệm trước Ủy ban nhân dân tỉnh trong việc bảo đảm an toàn thông tin trên địa bàn tỉnh.

2. Thực hiện theo dõi, đôn đốc, hướng dẫn, kiểm tra, giám sát công tác bảo đảm an ninh mạng, an toàn thông tin; thẩm định, phê duyệt hồ sơ cấp độ an toàn thông tin và phương án bảo đảm an toàn cho các hệ thống thông tin theo quy định của pháp luật và các văn bản hướng dẫn thi hành; ý kiến thẩm định, phê duyệt cấp độ an toàn hệ thống thông tin trong dự án đầu tư ứng dụng công nghệ thông tin theo quy định hiện hành.

3. Tham mưu Ủy ban nhân dân tỉnh đầu tư, triển khai các giải pháp kỹ thuật và ứng dụng công nghệ hiện đại, tiên tiến nhằm tăng cường hiệu quả công tác quản lý nhà nước, đồng thời chủ động phòng ngừa, phát hiện và xử lý các nguy cơ, sự cố về an toàn, an ninh thông tin mạng trên phạm vi toàn tỉnh.

4. Chủ trì, phối hợp với các cơ quan, đơn vị có liên quan xây dựng hướng dẫn nghiệp vụ về bảo đảm an ninh mạng, an toàn thông tin theo hướng cụ thể, chặt chẽ, dễ nhớ và dễ thực hiện, trong đó xác định rõ trách nhiệm, thời hạn và kết quả đầu ra.

5. Chủ trì, phối hợp với Sở Khoa học và công nghệ, các cơ quan, đơn vị có liên quan tiến hành kiểm tra, đánh giá công tác bảo đảm an ninh mạng, an toàn thông tin định kỳ hàng năm hoặc đột xuất khi có yêu cầu của cơ quan nhà nước có thẩm quyền.

6. Chủ trì, phối hợp với Sở Khoa học và công nghệ, các cơ quan, đơn vị có liên quan xây dựng kế hoạch phát hiện, đấu tranh, ngăn chặn tội phạm lợi dụng hệ thống thông tin gây phương hại đến an ninh quốc gia, gây mất an ninh trật tự và an ninh mạng, an toàn thông tin trong cơ quan nhà nước trên địa bàn tỉnh. Kịp thời thông báo các phương thức, thủ đoạn mới của các loại tội phạm công nghệ cao.

7. Hàng năm, xây dựng và triển khai các kế hoạch đào tạo, tập huấn về công tác bảo đảm an ninh mạng, an toàn thông tin cho cán bộ, công chức, viên chức chuyên trách về công nghệ thông tin; đào tạo, tập huấn chuyên sâu về an ninh mạng, an toàn thông tin cho lực lượng bảo đảm an ninh mạng, an toàn thông tin của các cơ quan, đơn vị; đào tạo, tập huấn, hướng dẫn về kiến thức, kỹ năng an toàn an ninh mạng cho tổ công nghệ số cộng đồng để phổ biến, hướng dẫn cho

người dân thực hiện. Tổ chức các hội nghị, hội thảo chuyên đề và tuyên truyền về an ninh mạng, an toàn thông tin trong công tác quản lý nhà nước trên địa bàn tỉnh.

8. Là cơ quan đầu mối, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin; tham mưu Ủy ban nhân dân tỉnh thành lập, kiện toàn Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh và tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an ninh mạng, an toàn thông tin trên địa bàn tỉnh.

9. Định kỳ hàng năm tổ chức diễn tập ứng cứu sự cố an ninh mạng, an toàn thông tin trên địa bàn tỉnh, tham gia diễn tập quốc gia và quốc tế do Bộ Công an, các đơn vị trong và ngoài nước tổ chức.

10. Tổng hợp và báo cáo về tình hình an ninh mạng, an toàn thông tin theo định kỳ cho Bộ Công an, Ủy ban nhân dân tỉnh và các cơ quan, đơn vị có liên quan. Đề nghị Ủy ban nhân dân tỉnh khen thưởng hoặc phê bình người đứng đầu cơ quan, đơn vị trong thực hiện chỉ đạo về bảo đảm an ninh mạng, an toàn thông tin.

11. Tham gia mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia và thực hiện trách nhiệm, quyền hạn của thành viên mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia theo quy định tại Quyết định số 05/2017/QĐ-TTg.

Điều 23. Trách nhiệm của Sở Khoa học và công nghệ

1. Chỉ đạo Trung tâm Chuyển đổi số tỉnh (đơn vị vận hành Trung tâm Dữ liệu tỉnh) triển khai thực hiện công tác giám sát, bảo đảm an ninh mạng, an toàn thông tin đối với các hệ thống thông tin đang cài đặt, vận hành tại Trung tâm Dữ liệu tỉnh, các hệ thống thông tin của các cơ quan, đơn vị có kết nối đến Trung tâm Dữ liệu tỉnh theo quy định; kịp thời cung cấp các thông tin, dữ liệu có liên quan cho các cơ quan chức năng có thẩm quyền để phục vụ công tác điều tra, xác minh an ninh mạng, an toàn thông tin khi có yêu cầu.

2. Phối hợp với Công an tỉnh trong công tác kiểm tra, đánh giá về an ninh mạng, an toàn thông tin.

3. 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.

4. Tham gia mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia và thực hiện trách nhiệm, quyền hạn của thành viên mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia theo quy định tại Quyết định số 05/2017/QĐ-TTg.

Điều 24. Trách nhiệm của Văn phòng UBND tỉnh

1. Quản trị, vận hành Hệ thống thông tin giải quyết thủ tục hành chính của tỉnh và triển khai thực hiện công tác bảo đảm an ninh mạng, an toàn thông tin theo quy định.

2. Quản trị, vận hành thống nhất Cổng thông tin điện tử dùng chung của tỉnh và các sở, ban, ngành, địa phương, đảm bảo đồng bộ về công nghệ và an toàn thông tin.

3. Kịp thời cung cấp các thông tin, dữ liệu có liên quan thuộc phạm vi quản lý cho các cơ quan chức năng có thẩm quyền để phục vụ công tác điều tra, xác minh khi có yêu cầu.

Điều 25. Trách nhiệm của Sở Tài chính

Trên cơ sở đề xuất của các cơ quan, đơn vị, địa phương và khả năng cân đối ngân sách, Sở Tài chính tham mưu cho cấp có thẩm quyền bố trí nguồn vốn đầu tư công thực hiện các dự án bảo đảm an ninh mạng, an toàn thông tin; phân bổ kinh phí chi thường xuyên ngân sách tỉnh thực hiện các nhiệm vụ bảo đảm an ninh mạng, an toàn thông tin theo quy định của Luật Ngân sách Nhà nước và các văn bản hướng dẫn có liên quan.

Điều 26. Trách nhiệm của Sở Nội vụ

1. Tham mưu Ủy ban nhân dân tỉnh có cơ chế chính sách để thu hút các chuyên gia về an toàn an ninh thông tin làm việc tại tỉnh. Bố trí cán bộ chuyên trách về an toàn an ninh thông tin trong các cơ quan, đơn vị để triển khai hiệu quả công tác bảo đảm an toàn hệ thống thông tin theo cấp độ, công tác bảo đảm an toàn thông tin theo mô hình 4 lớp, đặc biệt là đối với Trung tâm Dữ liệu tỉnh và các hệ thống thông tin quan trọng, dùng chung của tỉnh.

2. Phối hợp với Công an tỉnh, Sở Khoa học và công nghệ triển khai tổ chức các lớp đào tạo, bồi dưỡng nâng cao kiến thức về Chính quyền điện tử, Chính

quyền số, chuyển đổi số và bảo đảm an toàn, an ninh thông tin mạng cho cán bộ, công chức, viên chức, người lao động của tỉnh.

Điều 27. Trách nhiệm của các cơ quan, đơn vị

1. Chịu trách nhiệm trong công tác bảo đảm an ninh mạng, an toàn thông tin 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 an toàn thông tin và bảo đảm an toàn cho hệ thống thông tin của đơn vị quản lý theo quy định tại Luật An toàn thông tin mạng và các văn bản hướng dẫn thi hành.

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

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

5. Ban hành Quy định, quy trình nội bộ về bảo đảm an ninh mạng, an toàn thông tin gồm các nội dung cơ bản như quy định về quản lý hạ tầng mạng, bảo đảm an toàn dữ liệu, bảo đảm an toàn thiết bị và người dùng đầu cuối phù hợp với Quy định này và các quy định của pháp luật.

6. 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.

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

8. Hàng năm bố trí kinh phí cho việc ứng dụng công nghệ thông tin nói chung và công tác bảo đảm an ninh mạng, an toàn thông tin nói riêng trong nội bộ cơ quan, đơn vị mình; lập kế hoạch mua sắm bổ sung trang thiết bị, nâng cấp, bảo trì, sửa chữa, gia hạn bản quyền phần mềm, gia hạn bảo hành cho các hệ thống phần cứng, phần mềm nhằm thực hiện tốt công tác bảo mật, bảo đảm an ninh mạng, an toàn thông tin, đáp ứng các yêu cầu của phương án bảo đảm an toàn thông tin theo cấp độ được phê duyệt.

9. Thực hiện trình tự, thủ tục lập, trình thẩm định, phê duyệt cấp độ an toàn hệ thống thông tin trong dự án đầu tư ứng dụng công nghệ thông tin thực hiện theo quy định của pháp luật về an ninh mạng, an toàn thông tin.

10. 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 an toàn thông tin. Phân công lãnh đạo phụ trách công tác đảm bảo an toàn thông tin đối với các hệ thống thông tin và cơ sở dữ liệu do đơn vị quản lý

11. Thực hiện các báo cáo về an ninh mạng, an toàn thông tin theo yêu cầu, hướng dẫn của Công an tỉnh.

Điều 28. Trách nhiệm của đơn vị vận hành hệ thống thông tin

1. Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại Quy chế này và các nhiệm vụ do chủ quản hệ thống thông tin phân công.

2. Chỉ đạo, phân công các bộ phận kỹ thuật thuộc đơn vị (quản lý ứng dụng; quản lý dữ liệu; vận hành hệ thống thông tin; triển khai và hỗ trợ kỹ thuật) triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến hệ thống thông tin.

Điều 29. Trách nhiệm của Đội ứng cứu sự cố an toàn thông tin mạng

1. Triển khai các giải pháp nhằm hỗ trợ các cơ quan, đơn vị trên địa bàn tỉnh về công tác bảo đảm an ninh mạng, an toàn thông tin, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số.

2. Phối hợp kiểm tra an toàn thông tin, an ninh mạng đối với hệ thống thông tin của các cơ quan, đơn vị.

3. Điều phối các hoạt động ứng cứu sự cố về an ninh mạng, an toàn thông tin

và tổ chức ứng cứu sự cố an ninh mạng, an toàn thông tin tại các cơ quan, đơn vị trên địa bàn tỉnh.

Điều 30. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan, đơn vị

1. Trách nhiệm của cán bộ, công chức, viên chức chuyên trách về công nghệ thông tin tại cơ quan, đơn vị

a) Nghiêm túc chấp hành các Quy định, quy trình nội bộ và các quy định khác của pháp luật về an ninh mạng, an toàn thông tin. Chịu trách nhiệm về các hành vi làm mất an ninh mạng, an toàn thông tin 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 định, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an ninh mạng, an toàn thông tin.

c) Thực hiện việc giám sát, đánh giá, báo cáo người đứng đầu cơ quan, đơn vị các rủi ro mất an ninh mạng, an toàn thông tin và mức độ nghiêm trọng của các rủi ro đó.

d) Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an ninh mạng, an toàn thông tin.

e) Thường xuyên cập nhật nâng cao kiến thức, trình độ chuyên môn đáp ứng yêu cầu bảo đảm an ninh mạng, an toàn thông tin của đơn vị.

2. Công chức, viên chức 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.

3. Trách nhiệm của người sử dụng

a) Nghiêm túc chấp hành các Quy định, quy trình nội bộ và các quy định khác của pháp luật về an ninh mạng, an toàn thông tin. Chịu trách nhiệm bảo đảm an ninh mạng, an toàn thông tin 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 được giao sử dụng.

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

d) Tham gia các chương trình đào tạo, hội nghị, hội thảo về an ninh mạng, an toàn thông tin được cơ quan hoặc đơn vị chuyên môn tổ chức.

Điều 31. 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 hoạt động thực hiện ứng dụng công nghệ thông tin, giao dịch điện tử, chuyển đổi số của các cơ quan nhà nước trên địa bàn tỉnh Khánh Hòa phải tuân thủ Quy chế này và các quy định hiện hành của pháp luật về an toàn, an ninh thông tin mạng.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 32. Khen thưởng, kỷ luật

1. Định kỳ hằng năm hoặc đột xuất, Công an tỉnh căn cứ kết quả kiểm tra, đánh giá, báo cáo công tác bảo đảm an ninh mạng, an toàn thông tin của các cơ quan, đơn vị, đề xuất Ủy ban nhân dân tỉnh xem xét khen thưởng cho các cá nhân, đơn vị có nhiều thành tích trong công tác bảo đảm an ninh mạng, an toàn thông tin theo quy định hiện hành.

2. Tổ chức, cá nhân có hành vi vi phạm Quy chế này thì tùy theo tính chất, mức độ sẽ bị xử lý kỷ luật, bồi thường thiệt hại và chịu trách nhiệm theo quy định của pháp luật.

Điều 33. Điều khoản thi hành

1. Công an tỉnh có trách nhiệm theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy chế, báo cáo Ủy ban nhân dân tỉnh định kỳ hằng năm hoặc đột xuất theo yêu cầu của cơ quan có thẩm quyền.

2. Người đứng đầu các cơ quan, đơn vị trên địa bàn tỉnh và các đơn vị liên quan có trách nhiệm tổ chức triển khai thực hiện nghiêm Quy chế này trong phạm vi quản lý của mình.

3. Khuyến khích các cơ quan Đảng, Mặt trận tổ quốc, các cơ quan, đơn vị khác thực hiện các hoạt động ứng dụng và phát triển công nghệ thông tin, chuyển đổi số, an toàn thông tin, an ninh mạng trên địa bàn tỉnh Khánh Hòa áp dụng Quy chế này.

4. Trong quá trình thực hiện Quy chế, nếu có các vấn đề vướng mắc, phát sinh, cơ quan, đơn vị kịp thời phản ánh về Công an tỉnh để tổng hợp, báo cáo Ủy ban nhân dân tỉnh xem xét sửa đổi, bổ sung cho phù hợp./.