ỦY BAN NHÂN DÂN TỈNH ĐẮK LẮK	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 93 /2026/QĐ-UBND	*Đắk Lắk, ngày 22 tháng 8 năm 2026*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an ninh mạng trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Đắk Lắk

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 được sửa đổi, bổ sung bởi Luật số 87/2025/QH15;

Căn cứ Luật An ninh mạng số 116/2025/QH15;

Căn cứ Luật Bảo vệ bí mật nhà nước số 117/2025/QH15;

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

Căn cứ Luật Dữ liệu số 60/2024/QH15;

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

Căn cứ Luật Chuyển đổi số số 148/2025/QH15;

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

Căn cứ Nghị định số 147/2024/NĐ-CP của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng;

Căn cứ Nghị định số 68/2024/NĐ-CP của Chính phủ quy định về chữ ký số chuyên dùng công vụ;

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

Căn cứ Quyết định số 05/2017/QĐ-TTg 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 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 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 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 bảo đảm an toàn hệ thống thông tin theo cấp độ;

Theo đề nghị của Giám đốc Công an tỉnh tại Tờ trình số 369/TTr-CAT-PA05 ngày 31 tháng 7 năm 2026;

Ủy ban nhân dân ban hành Quyết định ban hành Quy chế bảo đảm an ninh mạng trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Đắk Lắk.

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an ninh mạng trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Đắk Lắk.

Điều 2. Hiệu lực thi hành

1. Quyết định này có hiệu lực thi hành từ ngày *03* tháng *9* năm 2026.

2. Bãi bỏ các văn bản:

a) Bãi bỏ toàn bộ Quyết định số 20/2016/QĐ-UBND ngày 17 tháng 5 năm 2016 của Ủy ban nhân dân tỉnh Đắk Lắk (cũ) ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Đắk Lắk;

b) Bãi bỏ các Điều 2, Điều 3, Điều 4 Quyết định số 11/2025/QĐ-UBND ngày 18 tháng 02 năm 2025 của Ủy ban nhân dân tỉnh Đắk Lắk (cũ) sửa đổi, bổ sung một số điều của Quy chế khai thác, sử dụng dữ liệu của cơ sở dữ liệu dùng chung trên địa bàn tỉnh Đắk Lắk ban hành kèm theo Quyết định số 01/2023/QĐ-UBND và Quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Đắk Lắk ban hành kèm theo Quyết định số 20/2016/QĐ-UBND.

Điều 3. Tổ chức thực hiện

1. Công an tỉnh chủ trì, theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy chế này.

2. Chánh Văn phòng Ủy ban nhân dân tỉnh, Giám đốc các sở, ban, ngành thuộc Ủy ban nhân dân tỉnh; Chủ tịch Ủy ban nhân dân các xã, phường; Thủ trưởng các cơ quan, đơn vị, tổ chức và cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Văn phòng Chính phủ;
- Bộ Công an;
- Cục kiểm tra văn bản và Tổ chức thi hành pháp luật, Bộ Tư pháp;
- Thường trực Tỉnh ủy;
- Thường trực HĐND tỉnh;
- Ủy ban Mặt trận Tổ quốc tỉnh;
- Đoàn Đại biểu Quốc hội tỉnh;
- Chủ tịch, các Phó Chủ tịch UBND tỉnh;
- Các sở, ban, ngành, đoàn thể của tỉnh;
- UBND các xã, phường;
- Trung tâm CN&CTTĐT tỉnh;
- Báo và Phát thanh, Truyền hình Đắk Lắk;
- Lưu: VT, NC (w.10b).

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

ỦY BAN NHÂN DÂN TỈNH ĐẮK LẮK

Hồ Thị Nguyên Thảo

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

QUY CHẾ
Bảo đảm an ninh mạng trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Đắk Lắk

(Ban hành kèm theo Quyết định số: 93 /2026/QĐ-UBND)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về công tác bảo đảm an ninh mạng trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh Đắk Lắk.

Điều 2. Đối tượng áp dụng

1. Các sở, ban, ngành; các tổ chức hành chính khác, đơn vị sự nghiệp công lập thuộc Ủy ban nhân dân tỉnh; Ủy ban nhân dân xã, phường; các tổ chức chính trị, tổ chức chính trị - xã hội và các cơ quan, tổ chức khác được giao quản lý, vận hành hoặc sử dụng hệ thống thông tin thuộc phạm vi quản lý của tỉnh (gọi chung là cơ quan, đơn vị).

2. Cán bộ, công chức, viên chức, người lao động đang làm việc trong các cơ quan, đơn vị quy định tại khoản 1 Điều này.

3. Các tổ chức, doanh nghiệp, cá nhân cung cấp sản phẩm, dịch vụ công nghệ thông tin, an toàn thông tin, an ninh mạng, điện toán đám mây, trung tâm dữ liệu, nền tảng số, dịch vụ số hoặc tham gia thiết kế, xây dựng, quản trị, vận hành, bảo trì, kết nối, tích hợp, chia sẻ dữ liệu đối với các hệ thống thông tin thuộc phạm vi quản lý của tỉnh (gọi chung là bên cung cấp dịch vụ).

4. Các tổ chức, cá nhân khác có liên quan đến công tác bảo đảm an ninh mạng trên địa bàn tỉnh.

Điều 3. Nguyên tắc bảo vệ an ninh mạng

1. Bảo vệ an ninh mạng tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật An ninh mạng số 116/2025/QH15.

2. Việc bảo vệ thông tin mật, thông tin thuộc danh mục bí mật nhà nước trên không gian mạng là nguyên tắc bắt buộc, được thực hiện tuyệt đối theo quy định của pháp luật về bảo vệ bí mật nhà nước và các quy định về bảo đảm an ninh mạng tại Quy chế này.

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

Điều 4. Xây dựng quy định bảo đảm an ninh mạng

1. Các cơ quan, đơn vị phải xây dựng quy định bảo đảm an ninh mạng phù hợp với hệ thống thông tin, cơ cấu tổ chức, yêu cầu quản lý và hoạt động của cơ quan, đơn vị mình. Quy định bảo đảm an ninh mạng được lãnh đạo có thẩm quyền ký ban hành và triển khai thực hiện trong toàn cơ quan, đơn vị.

2. Quy định bảo đảm an ninh mạng cần đáp ứng các yêu cầu an ninh mạng tương ứng với từng cấp độ của hệ thống thông tin và tiêu chuẩn, quy chuẩn kỹ thuật về an ninh mạng.

3. Quy định bảo đảm an ninh mạng thường xuyên được rà soát, sửa đổi, bổ sung nhằm bảo đảm sự đầy đủ, phù hợp với các quy định của pháp luật hiện hành về bảo đảm an ninh mạng.

Chương II
BẢO ĐẢM AN NINH MẠNG
Mục 1
QUẢN LÝ TÀI SẢN CÔNG NGHỆ THÔNG TIN

Điều 5. Tài sản công nghệ thông tin

1. Tài sản phần cứng: Thiết bị công nghệ thông tin, vật mang tin và các thiết bị phục vụ cho hoạt động của hệ thống thông tin, như: Máy chủ, máy tính, thiết bị lưu trữ (USB, Ổ cứng, CD/DVD, băng từ...); thiết bị mạng và bảo mật bộ định tuyến, bộ chuyển mạch, tường lửa vật lý, thiết bị cân bằng tải,...; thiết bị ngoại vi (máy in, máy quét,...); hệ thống cáp mạng; thiết bị cung cấp nguồn điện;...

2. Tài sản phần mềm: Phần mềm hệ thống, phần mềm ứng dụng, phần mềm tiện ích, hệ quản trị cơ sở dữ liệu, mã nguồn và công cụ phát triển phần mềm.

3. Tài sản thông tin: Dữ liệu, thông tin ở dạng số được tạo lập, thu thập, xử lý, lưu trữ, truyền đưa thông qua hệ thống thông tin.

4. Các thành phần liên quan khác.

Điều 6. Quản lý tài sản phần cứng

1. Với mỗi hệ thống thông tin, các cơ quan, đơn vị phải lập danh sách tài sản phần cứng gồm các thông tin cơ bản sau: Tên tài sản, địa chỉ mạng IP (đối với thiết bị đặt địa chỉ IP tĩnh), địa chỉ phần cứng MAC/ mã nhận diện serial, vị trí lắp đặt, chủ thể quản lý, mục đích sử dụng, hệ thống thông tin tương ứng, tình trạng sử dụng, thời gian ngừng hỗ trợ kỹ thuật của hãng (nếu có). Thực hiện kiểm kê, rà soát và cập nhật danh sách cho tất cả tài sản phần cứng định kỳ tối thiểu 02 lần/năm.

2. Tài sản phần cứng được giao, gắn trách nhiệm cho bộ phận hoặc cá nhân quản lý, sử dụng; được định kỳ bảo trì, bảo dưỡng; được bố trí, lắp đặt tại

các địa điểm an toàn và được bảo vệ để giảm thiểu những rủi ro do các đe dọa, hiểm họa từ môi trường và các xâm nhập trái phép.

3. Tài sản phần cứng thuộc hệ thống thông tin từ cấp độ 3 trở lên phải được kiểm tra, đánh giá an ninh, an toàn thông tin trước khi đưa vào sử dụng; bảo đảm về nguồn điện dự phòng, chống quá tải, sụt giảm điện áp, chống sét lan truyền và có hệ thống tiếp địa trong quá trình sử dụng.

4. Thông tin, dữ liệu lưu trữ trong tài sản phần cứng khi thanh lý, thay đổi mục đích sử dụng được tiêu hủy về mặt vật lý hoặc được xóa dữ liệu an toàn bảo đảm không có khả năng phục hồi. Trường hợp không thực hiện xóa, ghi đè dữ liệu, thực hiện biện pháp tiêu hủy cấu phần lưu trữ dữ liệu trên tài sản đó.

5. Không tự ý sửa chữa tài sản phần cứng ở các cơ sở, dịch vụ ngoài cơ quan, đơn vị. Trường hợp cấp bách phải sửa chữa ở các cơ sở bên ngoài, thì phải được sự đồng ý, phê duyệt của Thủ trưởng cơ quan, đơn vị đồng thời có biện pháp xóa dữ liệu an toàn hoặc lưu giữ lại bộ phận lưu trữ dữ liệu trước khi thực hiện sửa chữa. Trong quá trình sửa chữa, bảo trì hệ thống, thiết bị công nghệ thông tin do bên thứ ba thực hiện, đơn vị chủ quản, vận hành hệ thống thông tin phải cử bộ phận hoặc cán bộ chuyên trách/phụ trách về an ninh mạng giám sát và ghi nhật ký đầy đủ.

Điều 7. Quản lý tài sản phần mềm

1. Với mỗi hệ thống thông tin, các cơ quan, đơn vị lập danh sách tài sản phần mềm với các thông tin cơ bản gồm: tên tài sản, mục đích, phạm vi sử dụng, chủ thể quản lý, thông tin về bản quyền, phiên bản, hệ thống thông tin tương ứng. Thực hiện kiểm kê, rà soát và cập nhật danh sách cho tất cả tài sản phần mềm định kỳ tối thiểu 02 lần/năm.

2. Tài sản phần mềm phải được giao trách nhiệm cho bộ phận hoặc cá nhân quản lý, sử dụng; việc cài đặt, cấu hình, cập nhật, gia hạn bản quyền chỉ thực hiện bởi bộ phận hoặc người được giao nhiệm vụ theo quy định của cơ quan, đơn vị.

3. Cơ quan, đơn vị định kỳ rà soát, cập nhật, khắc phục các điểm yếu, lỗ hổng bảo mật có nguy cơ gây mất an ninh mạng.

Điều 8. Quản lý tài sản thông tin

1. Với mỗi hệ thống thông tin, các cơ quan, đơn vị phải lập danh sách tài sản thông tin với các thông tin cơ bản gồm: Tên tài sản, mức độ tiếp cận, chủ thể quản lý, phạm vi truy cập thông tin, thời gian lưu trữ, hệ thống thông tin tương ứng. Đánh giá và cập nhật danh sách tài sản thông tin tối thiểu 01 lần/năm hoặc khi xảy ra thay đổi trong cơ quan, đơn vị ảnh hưởng đến danh sách.

2. Thông tin được phân loại theo mức độ tiếp cận và có thể gắn thuộc tính đặc thù, cụ thể:

a) Thông tin phân loại theo mức độ công khai là thông tin được công khai cho tất cả các đối tượng mà không cần xác định danh tính, địa chỉ cụ thể của các đối tượng đó.

b) Thông tin phân loại theo mức độ nội bộ là thông tin được phân quyền quản lý, khai thác cho một hoặc một nhóm đối tượng đã được xác định danh tính, địa chỉ cụ thể.

c) Thông tin phân loại theo mức độ cá nhân là thông tin gắn với việc xác định danh tính một người cụ thể.

d) Thông tin phân loại theo mức độ bí mật nhà nước được quy định tại Luật Bảo vệ bí mật nhà nước số 117/2025/QH15.

3. Tài sản thông tin thuộc danh mục bí mật nhà nước phải tuân thủ các quy định của Luật số 117/2025/QH15, Luật Cơ yếu số 05/2011/QH13 và các quy định khác có liên quan đến quá trình tạo lập, lưu trữ, trao đổi và tiêu hủy.

Mục 2
XÂY DỰNG, QUẢN LÝ, VẬN HÀNH, HỦY BỎ HỆ THỐNG THÔNG TIN

Điều 9. Yêu cầu khi xây dựng các hệ thống thông tin

1. Khi xây dựng mới hoặc mở rộng, nâng cấp hệ thống thông tin, chủ quản hệ thống thông tin phải thực hiện xác định cấp độ hệ thống thông tin theo Nghị định số 85/2016/NĐ-CP về bảo đảm an toàn hệ thống thông tin theo cấp độ; đồng thời tuân thủ các quy định về phân loại và nhiệm vụ bảo vệ hệ thống thông tin tại Điều 8 và Điều 10 Luật số 116/2025/QH15.

2. Khi triển khai các sản phẩm bảo đảm an ninh mạng trong các hệ thống thông tin phải đáp ứng theo các tiêu chuẩn, quy chuẩn Việt Nam và các hướng dẫn về an ninh mạng của Bộ Công an, Công an tỉnh. Ưu tiên sử dụng sản phẩm, giải pháp và dịch vụ về an ninh mạng của các đơn vị, tổ chức trong nước.

Điều 10. Yêu cầu quản lý, vận hành, hủy bỏ hệ thống thông tin

1. Hệ thống thông tin phải có tài liệu hướng dẫn sử dụng; quy trình quản lý, vận hành; quy chế hoạt động; phương án bảo đảm an ninh mạng; kế hoạch ứng cứu sự cố an ninh mạng thể hiện vai trò, trách nhiệm của tổ chức, cá nhân trong quá trình quản lý, vận hành, sử dụng và ứng cứu sự cố.

2. Áp dụng các tiêu chuẩn, quy chuẩn kỹ thuật về an ninh mạng theo quy định của pháp luật để bảo đảm hoạt động bình thường đối với tất cả các hệ thống thông tin hiện có và các hệ thống thông tin mới trước khi đưa vào hoạt động chính thức.

3. Căn cứ các tiêu chuẩn, định mức, yêu cầu kỹ thuật theo quy định của pháp luật, tổ chức giám sát, tối ưu hiệu suất của hệ thống thông tin; đánh giá khả năng đáp ứng, tình trạng hoạt động, cấu hình hệ thống của hệ thống thông tin để

dự báo, lập kế hoạch mở rộng, nâng cấp bảo đảm khả năng đáp ứng về an ninh mạng hệ thống thông tin trong tương lai.

4. Quản lý nhật ký trong quá trình vận hành các hệ thống thông tin:

a) Các cơ quan, đơn vị phải thực hiện việc ghi nhật ký (log) trên các thiết bị mạng máy tính, phần mềm ứng dụng, hệ điều hành, cơ sở dữ liệu nhằm bảo đảm các sự kiện quan trọng xảy ra trên hệ thống được ghi nhận, lưu giữ và bảo vệ nhằm phục vụ công tác phân tích, kiểm tra, điều tra, giám sát an ninh mạng.

b) Các sự kiện tối thiểu cần phải được ghi nhật ký gồm: quá trình đăng nhập hệ thống; tạo, cập nhật hoặc xóa dữ liệu; các hành vi xem, thiết lập cấu hình hệ thống; việc thiết lập các kết nối bất thường vào và ra hệ thống; thay đổi quyền truy cập hệ thống.

c) Thường xuyên thực hiện việc theo dõi bản ghi nhật ký của hệ thống và các sự kiện khác có liên quan để đánh giá, báo cáo các rủi ro và mức độ nghiêm trọng các rủi ro đó, đồng thời, kết nối, chia sẻ nhật ký về Trung tâm An ninh mạng tỉnh (nếu có) để giám sát.

5. Hủy bỏ hệ thống thông tin do chủ quản hệ thống thông tin quyết định bằng văn bản và thông báo đến các tổ chức, cá nhân liên quan và đơn vị chuyên trách an ninh mạng của tỉnh. Quá trình hủy bỏ thực hiện theo phương án bảo đảm an ninh mạng đã được phê duyệt; trước khi hủy bỏ, phải sao lưu toàn bộ dữ liệu, cấu hình và nhật ký để phục vụ công tác tra cứu, lưu trữ và quản lý tài sản công nghệ thông tin của hệ thống theo quy định của pháp luật.

Điều 11. Quản lý thuê dịch vụ công nghệ thông tin

1. Xác định rõ phạm vi, trách nhiệm, quyền hạn và nghĩa vụ của các bên về bảo đảm an ninh mạng, bảo vệ bí mật nhà nước, bảo vệ dữ liệu, dữ liệu cá nhân và xử lý vi phạm, trách nhiệm bồi thường, khắc phục thiệt hại do hành vi vi phạm của bên cung cấp dịch vụ gây ra trước khi ký kết hợp đồng thuê.

2. Trách nhiệm của cơ quan, đơn vị chủ trì trong quá trình thuê dịch vụ công nghệ thông tin:

a) Quản lý chặt chẽ thông tin, dữ liệu phát sinh từ dịch vụ thuê, chỉ cho phép truy nhập trong phạm vi được cấp quyền và chịu sự giám sát của cơ quan chủ quản.

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 an ninh mạng theo quy định tại Quy chế này 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 an ninh mạng 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, khắc phục thiệt hại.

đ) Phối hợp với bên cung cấp dịch vụ trong việc lập, hoàn thiện hồ sơ đề xuất cấp độ hệ thống thông tin theo quy định; yêu cầu bên cung cấp dịch vụ cung cấp đầy đủ tài liệu thiết kế, cấu hình, phương án kỹ thuật 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 Khung kiến trúc Chính phủ số Việt Nam; Khung kiến trúc số tỉnh Đắk Lắk và các tiêu chuẩn, quy chuẩn kỹ thuật có liên quan.

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

a) Thu hồi quyền truy cập hệ thống thông tin và các tài sản công nghệ thông tin 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. Có phương án hợp đồng chặt chẽ với bên 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 bên cung cấp dịch vụ, tránh tình trạng ủy quyền toàn bộ việc quản trị, vận hành hệ thống cho bên cung cấp dịch vụ liên quan đến khai thác, sử dụng cơ sở dữ liệu hệ thống.

5. Bên 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 các hệ thống thông tin quan trọng về an ninh quốc gia cần báo cáo về Công an tỉnh để phối hợp đơn vị nghiệp vụ Bộ Công an thực hiện kiểm tra an ninh thông tin bảo đảm đáp ứng các tiêu chí theo hướng dẫn của Bộ Công an, chủ quản hệ thống thông tin quan trọng quốc gia và quy định pháp luật.

Điều 12. Quản lý Trung tâm dữ liệu/Phòng máy chủ

1. Các thiết bị tường lửa, máy chủ, hệ thống lưu trữ... phải được đặt trong Trung tâm dữ liệu/Phòng máy chủ và thiết lập cơ chế bảo vệ, theo dõi phát hiện xâm nhập và biện pháp kiểm soát truy cập vật lý phù hợp.

2. Máy chủ phải được cài đặt phần mềm phòng chống mã độc và quản lý thống nhất, tập trung. Nhật ký hoạt động của thiết bị, phần mềm bảo đảm thời gian lưu giữ theo đúng cấp độ an toàn của hệ thống thông tin.

3. Mang thiết bị vào, ra Trung tâm dữ liệu/Phòng máy chủ để lắp đặt hoặc sửa chữa phải có sự chấp thuận của thủ trưởng cơ quan, đơn vị quản lý, vận hành.

Điều 13. Quản lý Hệ thống mạng máy tính

1. Hệ thống mạng máy tính phải được thiết kế phân vùng theo chức năng và mức độ an ninh phù hợp với từng cấp độ an ninh mạng của hệ thống thông tin theo TCVN 11930:2017 về Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ. Dữ liệu trao đổi giữa các vùng mạng phải được kiểm soát chặt chẽ bởi thiết bị tường lửa và các thiết bị bảo mật khác.

2. Hệ thống mạng máy tính kết nối Internet phải có hệ thống tường lửa, hệ thống bảo vệ truy cập Internet và có khả năng bảo vệ trước các loại tấn công từ chối dịch vụ (DDoS); thực hiện lọc bỏ, ngăn chặn truy cập các trang tin được xác định là chứa mã độc hoặc nội dung không phù hợp.

3. Truy cập từ xa vào vùng mạng nội bộ phải thông qua kết nối mạng riêng ảo (VPN) được mã hóa, có kiểm soát và áp dụng hình thức xác thực đa yếu tố (MFA).

4. Kết nối không dây (Wi-Fi) phải sử dụng chế độ xác thực mạnh (như WPA2- Enterprise) hoặc mật khẩu mạnh, thay đổi định kỳ. Đối với vùng mạng nội bộ phải thực hiện quản lý thiết bị kết nối Wi-Fi theo địa chỉ phần cứng MAC của thiết bị.

5. Điểm truy nhập Internet công cộng tại cơ quan, đơn vị phải niêm yết công khai nội quy sử dụng dịch vụ Internet ở nơi dễ nhận biết; thiết lập thành vùng mạng riêng biệt, không kết nối vùng mạng nội bộ chứa dữ liệu chuyên môn; thiết lập mật khẩu mạnh, khuyến khích sử dụng cổng xác thực (Captive Portal) yêu cầu người dùng chấp nhận nội quy sử dụng trước khi truy cập Internet qua Wi-Fi.

6. Mạng truyền số liệu chuyên dùng trên địa bàn tỉnh được triển khai, quản lý, vận hành và sử dụng phải tuân thủ các quy định của Thủ tướng Chính phủ và hướng dẫn của Bộ Khoa học và Công nghệ, Ban Cơ yếu Chính phủ. Chỉ được sử dụng cho mục đích công vụ, không được kết nối trực tiếp ra Internet.

Điều 14. Quản lý, sử dụng máy tính, thiết bị ngoại vi và phần mềm

1. Máy tính và các thiết bị ngoại vi tại các cơ quan, đơn vị phải được cài đặt hệ điều hành, phần mềm ứng dụng có bản quyền hoặc sử dụng phần mềm mã nguồn mở hợp pháp, có nguồn gốc rõ ràng.

2. Chỉ cài đặt các phần mềm nằm trong danh mục được phép sử dụng do cơ quan có thẩm quyền ban hành (nếu có). Nghiêm cấm việc tự ý cài đặt các

phần mềm không rõ nguồn gốc, phần mềm bẻ khóa, các phần mềm không phục vụ công tác chuyên môn hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận hoặc cán bộ chuyên trách/phụ trách về an ninh mạng của cơ quan, đơn vị.

3. Tất cả các máy tính phải được cài đặt phần mềm phòng, chống mã độc và được thiết lập chế độ cập nhật tự động cơ sở dữ liệu nhận dạng mã độc, bản vá cho hệ điều hành và phần mềm. Người sử dụng có trách nhiệm thường xuyên rà quét mã độc đối với máy tính và các thiết bị lưu trữ di động (USB, Ổ cứng ngoài) trước khi sử dụng.

4. Khi phát hiện máy tính có dấu hiệu bất thường (hoạt động chậm, tự động mở các cửa sổ lạ, mất dữ liệu, nhận được cảnh báo từ phần mềm phòng, chống mã độc), người sử dụng phải ngay lập tức ngắt kết nối mạng của máy tính đó và báo cáo cho bộ phận hoặc cán bộ chuyên trách/phụ trách về an ninh mạng của cơ quan, đơn vị để được hỗ trợ, xử lý kịp thời.

5. 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 phổ biến; không truy nhập, mở các trang tin, tệp đính kèm hoặc liên kết trong thư điện tử không rõ nguồn gốc, có dấu hiệu đáng ngờ; thực hiện quét mã độc của tệp đính kèm tải về trước khi mở ra xem; không sử dụng tính năng lưu mật khẩu tự động hoặc đăng nhập tự động.

6. Người sử dụng phải khóa màn hình máy tính (sử dụng tính năng có sẵn của hệ điều hành) khi rời khỏi vị trí làm việc và tắt hoàn toàn máy tính khi hết giờ làm việc.

Điều 15. Quản lý, sử dụng chữ ký số, chứng thư chữ ký số chuyên dùng

1. Chữ ký số chuyên dùng công vụ và chứng thư chữ ký số chuyên dùng công vụ sử dụng trong hoạt động công vụ của các cơ quan, đơn vị được quản lý, cung cấp bởi tổ chức cung cấp dịch vụ chứng thực chữ ký số chuyên dùng công vụ theo quy định của pháp luật về giao dịch điện tử, pháp luật về cơ yếu và pháp luật có liên quan.

2. Cá nhân được cấp chữ ký số, chứng thư chữ ký số chuyên dùng chịu trách nhiệm quản lý, bảo vệ an ninh, bí mật khóa bí mật và thiết bị lưu khóa bí mật.

3. Nghiêm cấm việc cho người khác mượn thiết bị lưu khóa bí mật hoặc sử dụng chữ ký số được cấp vào các mục đích cá nhân, không phục vụ công vụ.

4. Tổ chức, cá nhân được cấp chứng thư chữ ký số chuyên dùng công vụ thực hiện nghiêm túc trách nhiệm của thuê bao quy định tại Điều 39 Nghị định số 68/2024/NĐ-CP quy định về chữ ký số chuyên dùng công vụ.

Điều 16. Quản lý tài khoản và quyền truy cập tài khoản của người dùng

1. Mỗi cá nhân, đơn vị được cấp một tài khoản định danh duy nhất từ Hệ thống định danh và xác thực tập trung của tỉnh để truy cập các hệ thống thông tin dùng chung của tỉnh.

2. Mỗi tài khoản truy cập các hệ thống thông tin chỉ được giao cho một người quản lý, sử dụng và chịu trách nhiệm chính về bảo mật tài khoản, thông tin xác thực và hoạt động truy cập tài khoản. Việc sử dụng chung tài khoản bị nghiêm cấm.

3. Mỗi người sử dụng chỉ được phép truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình, có trách nhiệm bảo mật tài khoản truy cập thông tin.

4. Tài khoản người dùng phải đặt mật khẩu mạnh và thay đổi định kỳ tối thiểu 90 ngày/lần. Hệ thống có cơ chế xác thực người dùng; bắt buộc người dùng thay đổi mật khẩu ngay trong lần đăng nhập đầu tiên; tự động khóa tài khoản tạm thời sau 05 lần đăng nhập sai liên tiếp.

5. Tài khoản quản trị, vận hành hệ thống phải tách biệt với tài khoản truy cập của người sử dụng thông thường, được giao đích danh cá nhân làm công tác quản trị và phải đặt mật khẩu mạnh tối thiểu 14 ký tự. Hệ thống có cơ chế xác thực 02 yếu tố; thay đổi mật khẩu định kỳ tối thiểu 90 ngày/lần; tự động khóa tài khoản tạm thời sau 05 lần đăng nhập sai liên tiếp; hiển thị lịch sử đăng nhập thành công của mỗi tài khoản và thông báo về tài khoản quản trị.

6. Đơn vị quản lý, vận hành hệ thống thông tin có quyền khóa tài khoản truy cập trong trường hợp khi không tuân thủ các quy định về an ninh mạng hoặc phát hiện tài khoản đó có hành vi tấn công mạng hoặc gây mất an ninh mạng.

Điều 17. Bảo đảm an ninh dữ liệu; sao lưu dự phòng và khôi phục

1. Cơ quan, đơn vị xây dựng và tổ chức thực hiện chính sách/quy trình quản lý dữ liệu (phân loại dữ liệu, phân quyền truy cập, lưu trữ, sao lưu, khôi phục, tiêu hủy), bảo đảm tính bí mật, tính toàn vẹn và tính sẵn sàng, trong đó tối thiểu bao gồm: kiểm soát truy cập, ghi nhật ký, mã hóa phù hợp đối với dữ liệu quan trọng/nhạy cảm khi lưu trữ và khi truyền nhận, quản lý khóa mã hóa theo thẩm quyền. Các cơ quan, đơn vị khi thuê dịch vụ cần yêu cầu bên 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.

2. Khuyến khích triển khai các giải pháp tăng tính sẵn sàng cho lưu trữ như RAID/nhân bản/cluster… để giảm gián đoạn dịch vụ, lưu ý các cơ chế này không thay thế sao lưu.

3. Đối với công tác sao lưu dự phòng và khôi phục dữ liệu (tần suất sao lưu dự phòng, phương tiện lưu trữ, thời gian lưu trữ, nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ):

a) Lập danh sách các dữ liệu, phần mềm cần được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu;

b) Xây dựng tài liệu, quy trình hướng dẫn sao lưu/phục hồi dữ liệu: Đơn vị chủ quản hệ thống thông tin thực hiện xây dựng tài liệu hướng dẫn sao lưu cụ thể đối với từng hệ thống cung cấp dịch vụ, hệ thống điều hành mà đơn vị quản lý.

4. Bộ phận hoặc cán bộ chuyên trách/phụ trách về an ninh mạng phối hợp với các cơ quan, đơn vị có liên quan thực hiện phân loại tài sản thông tin, phần mềm, thực hiện quy trình sao lưu dự phòng và phục hồi cho các phần mềm, dữ liệu cần thiết theo quy định, quy trình sao lưu, lưu trữ hiện có. Các nội dung thực hiện gồm: Lập danh sách các dữ liệu (thông tin cấu hình của mạng, máy chủ), phần mềm ứng dụng, cơ sở dữ liệu, tệp tin ghi nhật ký hệ thống được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu; thực hiện quy trình sao lưu dự phòng và phục hồi.

5. Dữ liệu sao lưu phải được lưu giữ 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).

6. Khi thực hiện chia sẻ tài nguyên trên máy chủ hoặc máy trạm, đơn vị vận hành hệ thống thông tin phải sử dụng mật khẩu để bảo vệ thông tin, dữ liệu; không thực hiện chia sẻ toàn bộ ổ cứng; theo dõi, giám sát để kết thúc chia sẻ tài nguyên ngay khi hoàn thành. Các thông tin, tài liệu, dữ liệu nhạy cảm phải được mã hóa trước khi trao đổi, truyền nhận qua mạng máy tính.

7. Thông tin, dữ liệu thuộc phạm vi bí mật nhà nước thực hiện theo pháp luật về bảo vệ bí mật nhà nước; dữ liệu cá nhân thực hiện theo pháp luật về bảo vệ dữ liệu cá nhân và văn bản hướng dẫn thi hành.

Điều 18. Bảo đảm an ninh mạng đối với người sử dụng

1. Các cơ quan, đơn vị phải xây dựng các yêu cầu, trách nhiệm bảo đảm an ninh mạng đối với từng vị trí công việc. Sau khi tuyển dụng, tiếp nhận nhân sự mới, cơ quan, đơn vị phải có trách nhiệm phổ biến cho nhân sự mới các quy định về bảo đảm an ninh mạng đối với từng hệ thống thông tin được quản lý, sử dụng; đối với các vị trí tiếp xúc, quản lý các thông tin, dữ liệu quan trọng hoặc quản trị các hệ thống thông tin quan trọng, cơ quan, đơn vị phải yêu cầu nhân sự mới cam kết bảo mật thông tin bằng văn bản hoặc cam kết trong hợp đồng làm việc, hợp đồng lao động.

2. Các cơ quan, đơn vị phải xây dựng quy trình cấp mới, quản lý và thu hồi tài khoản, phân quyền truy cập các hệ thống thông tin và tất cả các tài sản công nghệ thông tin liên quan đến hệ thống thông tin đối với các cá nhân do cơ quan, đơn vị quản lý. Người sử dụng phải kiểm tra thông tin, dữ liệu được lưu giữ trên các tài sản công nghệ thông tin trước khi tiếp nhận.

3. Khi cá nhân chấm dứt hoặc thay đổi công việc, cơ quan, đơn vị có trách nhiệm:

a) Xác định rõ trách nhiệm của cán bộ, công chức, viên chức, người lao động và các bên liên quan trong quản lý, sử dụng các tài sản công nghệ thông tin được giao.

b) Lập biên bản bàn giao tài sản công nghệ thông tin.

c) Thay đổi hoặc thu hồi quyền truy cập các hệ thống thông tin.

4. Việc kết nối thiết bị thuộc sở hữu cá nhân (máy tính xách tay, điện thoại thông minh, máy tính bảng…) vào vùng mạng nội bộ của cơ quan, đơn vị để xử lý công việc phải được sự đồng ý của thủ trưởng cơ quan, đơn vị và phải tuân thủ các quy định về bảo đảm an ninh mạng được quy định tại quy chế này; chịu sự giám sát của bộ phận hoặc cán bộ chuyên trách/phụ trách về an ninh mạng của cơ quan, đơn vị.

Điều 19. Đào tạo, bồi dưỡng nghiệp vụ, tuyên truyền, phổ biến kiến thức về an ninh mạng

1. Các cơ quan, đơn vị phải tổ chức tập huấn, hướng dẫn quản lý, sử dụng hệ thống thông tin bảo đảm an ninh mạng trước khi triển khai chính thức hoặc sau khi nâng cấp hệ thống.

2. Các cơ quan, đơn vị xác định nhu cầu đào tạo cho nguồn nhân lực về bảo đảm an ninh mạng tại cơ quan, đơn vị mình gửi Sở Nội vụ, Công an tỉnh tổng hợp, tham mưu tổ chức đào tạo.

3. Các cơ quan, đơn vị cử cán bộ tham gia hoặc phối hợp tổ chức đào tạo, bồi dưỡng kiến thức về an ninh mạng khi cần thiết.

4. Các cơ quan, đơn vị phải thường xuyên tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức về bảo đảm an ninh mạng đến toàn thể cán bộ, công chức, viên chức và người lao động tại cơ quan, đơn vị.

Mục 3
BẢO ĐẢM HỆ THỐNG THÔNG TIN THEO CẤP ĐỘ

Điều 20. Phân loại và xác định cấp độ hệ thống thông tin

1. Tất cả các hệ thống thông tin do các cơ quan, đơn vị trong tỉnh quản lý, vận hành phải được phân loại và xác định cấp độ hệ thống thông tin để áp dụng các biện pháp quản lý và kỹ thuật tương ứng nhằm bảo vệ hệ thống thông tin.

2. Việc phân loại cấp độ hệ thống thông tin được thực hiện theo 5 cấp độ, từ cấp độ 1 đến cấp độ 5, dựa trên các tiêu chí quy định từ Điều 7 đến Điều 11 của Nghị định số 85/2016/NĐ-CP.

3. Chủ quản hệ thống thông tin có trách nhiệm chủ trì, chỉ đạo đơn vị vận hành hệ thống thông tin thực hiện việc xác định và đề xuất cấp độ cho các hệ thống thông tin thuộc phạm vi quản lý của mình.

Điều 21. Lập, thẩm định và phê duyệt hồ sơ đề xuất cấp độ hệ thống thông tin

1. Đơn vị vận hành hệ thống thông tin có trách nhiệm lập hồ sơ đề xuất cấp độ hệ thống thông tin theo quy định tại Điều 15 của Nghị định số 85/2016/NĐ-CP, bao gồm: Tài liệu mô tả tổng quan về hệ thống thông tin, thiết kế hệ thống thông tin, thuyết minh đề xuất cấp độ hệ thống thông tin, thuyết minh phương án bảo đảm an ninh mạng hệ thống thông tin.

2. Thẩm quyền thẩm định và phê duyệt cấp độ hệ thống thông tin:

a) Đối với hệ thống thông tin được đề xuất cấp độ 1 hoặc cấp độ 2: Công an tỉnh thực hiện việc hướng dẫn, kiểm tra, cho ý kiến chuyên môn, thẩm định hoặc tham mưu cấp có thẩm quyền phê duyệt hồ sơ đề xuất cấp độ hệ thống thông tin trong phạm vi nhiệm vụ được Ủy ban nhân dân tỉnh giao và theo quy định của pháp luật.

b) Đối với hệ thống thông tin được đề xuất cấp độ 3: Công an tỉnh chủ trì thẩm định hồ sơ đề xuất cấp độ. Ủy ban nhân dân tỉnh phê duyệt hồ sơ đề xuất cấp độ an ninh mạng trên cơ sở ý kiến thẩm định của Công an tỉnh.

c) Đối với hệ thống thông tin được đề xuất cấp độ 4 hoặc cấp độ 5, việc lập, thẩm định, phê duyệt hồ sơ đề xuất cấp độ và phương án bảo đảm an ninh mạng được thực hiện theo quy định của pháp luật. Công an tỉnh hướng dẫn, phối hợp với chủ quản hệ thống thông tin hoàn thiện hồ sơ và thực hiện các thủ tục thuộc trách nhiệm của địa phương.

3. Phối hợp trong quá trình thẩm định hồ sơ đề xuất cấp độ: Trong quá trình thẩm định hồ sơ đề xuất cấp độ, Công an tỉnh được lấy ý kiến Sở Khoa học và Công nghệ đối với các nội dung liên quan đến kiến trúc hệ thống, giải pháp kỹ thuật, hạ tầng số, nền tảng số dùng chung của tỉnh.

Điều 22. Phương án bảo đảm an ninh mạng theo cấp độ

1. Chủ quản hệ thống thông tin có trách nhiệm yêu cầu đơn vị vận hành xây dựng và triển khai đầy đủ phương án bảo đảm an ninh mạng đã được phê duyệt trong hồ sơ đề xuất cấp độ.

2. Phương án bảo đảm an ninh mạng phải đáp ứng các yêu cầu về quản lý, kỹ thuật tương ứng với cấp độ đã được phê duyệt, bao gồm các nội dung chính theo quy định tại Điều 19 Nghị định số 85/2016/NĐ-CP và các điều kiện an ninh mạng theo Tiêu chuẩn quốc gia TCVN 11930:2017 về Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ, TCVN 14423:2025 về An ninh mạng - Yêu cầu đối với hệ thống thông tin quan trọng.

3. Công an tỉnh có trách nhiệm hướng dẫn, đôn đốc, kiểm tra việc triển khai phương án bảo đảm an ninh mạng tại các cơ quan, đơn vị.

Điều 23. Bảo đảm an ninh mạng cho hệ thống thông tin quan trọng về an ninh quốc gia trên địa bàn tỉnh

1. Các cơ quan, đơn vị có trách nhiệm rà soát, xác định các hệ thống thông tin thuộc phạm vi quản lý có đủ tiêu chuẩn, khả năng thuộc danh mục quan trọng cần ưu tiên bảo đảm an ninh mạng và lập hồ sơ đề nghị đưa vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia theo quy định.

2. Việc bảo đảm an ninh mạng cho Hệ thống thông tin quan trọng về an ninh quốc gia phải được ưu tiên hàng đầu, được đầu tư nguồn lực tương xứng và áp dụng các biện pháp quản lý, kỹ thuật tăng cường.

3. Đơn vị chủ quản hệ thống thông tin quan trọng về an ninh quốc gia phải tổ chức triển khai đầy đủ các giải pháp bảo đảm an ninh mạng theo TCVN 14423:2025 về An ninh mạng - Yêu cầu đối với hệ thống thông tin quan trọng. Kết nối vào Trung tâm An ninh mạng quốc gia và Trung tâm An ninh mạng tỉnh (nếu có), chia sẻ dữ liệu, giám sát liên tục 24/7.

Mục 4
KIỂM TRA, GIÁM SÁT, CẢNH BÁO VÀ ỨNG CỨU SỰ CỐ

Điều 24. Kiểm tra, đánh giá an ninh mạng

1. Chủ quản hệ thống thông tin có thẩm quyền yêu cầu kiểm tra, đánh giá đối với các hệ thống thông tin thuộc thẩm quyền quản lý. Đơn vị chuyên trách về an ninh mạng của chủ quản hệ thống thông tin có thẩm quyền yêu cầu kiểm tra, đánh giá đối với các hệ thống thông tin do đơn vị này phê duyệt hồ sơ đề xuất cấp độ.

2. 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 việc kiểm tra, đánh giá. Đối tượng kiểm tra, đánh giá là chủ quản hệ thống thông tin hoặc đơn vị vận hành hệ thống thông tin và các hệ thống thông tin có liên quan.

3. Hoạt động kiểm tra, đánh giá an ninh mạng được thực hiện định kỳ hoặc đột xuất nhằm xác định thực trạng hệ thống thông tin; phát hiện, cảnh báo, khắc phục các lỗ hổng, điểm yếu bảo mật và đánh giá sự tuân thủ các quy định.

4. Việc kiểm tra, đánh giá được thực hiện theo quy định tại điểm c khoản 2 Điều 20 Nghị định số 85/2016/NĐ-CP, như sau:

a) Định kỳ 02 năm đối với hệ thống thông tin cấp độ 1 và cấp độ 2.

b) Định kỳ hằng năm đối với hệ thống thông tin cấp độ 3 và cấp độ 4.

c) Định kỳ 06 tháng một lần đối với hệ thống thông tin cấp độ 5.

5. Nội dung, hình thức kiểm tra, đánh giá quy định tại Điều 11, Điều 12 Thông tư số 12/2022/TT-BTTTT 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 bảo đảm an toàn hệ thống thông tin theo cấp độ và quy định có liên quan. Đơn vị chuyên trách về an ninh mạng có trách nhiệm thông báo kế hoạch, thành lập đoàn kiểm tra, lập biên bản và thông báo kết quả kiểm tra, đánh giá cho đơn vị được kiểm tra, đánh giá.

6. Cơ quan, đơn vị được kiểm tra có trách nhiệm phối hợp, cung cấp thông tin, tài liệu, nhật ký cần thiết, tạo điều kiện cho đoàn kiểm tra; tổ chức khắc phục các tồn tại theo yêu cầu và báo cáo kết quả khắc phục theo thời hạn được thông báo.

Điều 25. Giám sát, cảnh báo an ninh mạng

1. Các hệ thống thông tin phải được giám sát, cảnh báo an ninh mạng phù hợp với cấp độ, phạm vi, quy mô, tính chất xử lý thông tin; hệ thống từ cấp độ 3 trở lên và hệ thống quan trọng cần ưu tiên giám sát thường xuyên, liên tục theo quy định. Đơn vị vận hành hệ thống thông tin có trách nhiệm phối hợp với Công an tỉnh tổ chức thực hiện việc giám sát hệ thống thông tin theo Thông tư số 31/2017/TT-BTTTT quy định hoạt động giám sát an toàn hệ thống thông tin.

2. Các cơ quan, đơn vị là chủ quản hệ thống thông tin có trách nhiệm triển khai giải pháp giám sát an ninh mạng cho các hệ thống thuộc phạm vi quản lý (có thể tự triển khai hoặc thuê dịch vụ chuyên nghiệp).

3. Các hệ thống thông tin của các cơ quan, đơn vị phải được kết nối, chia sẻ thông tin, dữ liệu giám sát về Trung tâm An ninh mạng tỉnh (nếu có) để thực hiện giám sát tập trung, phân tích, cảnh báo sớm các nguy cơ, mối đe dọa trên toàn tỉnh và kết nối, chia sẻ kết quả giám sát về Trung tâm An ninh mạng quốc gia (thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Bộ Công an).

4. Trung tâm Giám sát, điều hành đô thị thông minh Đắk Lắk (đơn vị vận hành Trung tâm dữ liệu tỉnh) thực hiện giám sát kỹ thuật đối với các hệ thống đặt tại hạ tầng dùng chung của tỉnh; Công an tỉnh chủ trì công tác giám sát an ninh mạng theo chức năng, nhiệm vụ được giao.

Điều 26. Ứng cứu sự cố an ninh mạng

1. Đội ứng cứu sự cố an ninh mạng tỉnh do đơn vị chuyên trách an ninh mạng tỉnh (Công an tỉnh) tham mưu Ủy ban nhân dân tỉnh thành lập, kiện toàn có vai trò đầu mối điều phối các hoạt động ứng cứu sự cố trên toàn tỉnh.

2. Chủ quản hệ thống thông tin thành lập hoặc chỉ định bộ phận là Đội ứng cứu sự cố an ninh mạng nội bộ để thực hiện nhiệm vụ giám sát, phát hiện, xử lý và phối hợp khắc phục sự cố an ninh mạng trong phạm vi quản lý.

3. Khi ứng cứu sự cố an ninh mạng phải ưu tiên xử lý tại chỗ bằng lực lượng của chủ quản hệ thống thông tin và đơn vị vận hành hệ thống thông tin. Khi sự cố an ninh mạng vượt quá khả năng, Đội ứng cứu sự cố an ninh mạng nội

bộ tham mưu chủ quản hệ thống thông tin báo cáo ngay cho Công an tỉnh để kích hoạt cơ chế điều phối.

4. Phương án, kế hoạch ứng cứu sự cố an ninh mạng:

a) Công an tỉnh tham mưu Ủy ban nhân dân tỉnh ban hành, triển khai phương án ứng cứu sự cố an ninh mạng trên địa bàn tỉnh.

b) Đội ứng cứu sự cố an ninh mạng nội bộ tham mưu chủ quản hệ thống thông tin ban hành, triển khai kế hoạch ứng cứu sự cố an ninh mạng cho các hệ thống thông tin theo cấp độ được phê duyệt.

Điều 27. Quy trình ứng cứu sự cố an ninh mạng

1. Quy trình ứng cứu sự cố an ninh mạng tuân thủ quy định tại Quyết định số 05/2017/QĐ-TTg ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia, Thông tư số 20/2017/TT-BTTTT quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc; xác định yêu cầu về chất lượng dịch vụ và các nội dung đặc thù của hợp đồng thuê dịch vụ đối với thuê dịch vụ công nghệ thông tin theo yêu cầu riêng và phương án ứng cứu sự cố an ninh mạng của tỉnh, bao gồm: Phát hiện, tiếp nhận, phân loại, xử lý ban đầu, phân tích, khắc phục, điều tra và tổng kết, đánh giá.

2. Hoạt động của Đội ứng cứu sự cố an ninh mạng nội bộ:

a) Chủ động rà soát các lỗ hổng, điểm yếu bảo mật của hệ thống thông tin trong phạm vi quản lý và triển khai các giải pháp để khắc phục các nguy cơ này.

b) Tiếp nhận thông tin về sự cố từ hệ thống giám sát, người dùng hoặc thông báo từ cơ quan, đơn vị khác.

c) Kích hoạt quy trình ứng cứu, phân công nhiệm vụ và triển khai các biện pháp đánh giá, xử lý sự cố ban đầu; yêu cầu hỗ trợ, điều phối ứng cứu sự cố khi vượt khả năng.

d) Tổ chức thực hiện theo hướng dẫn của lực lượng chuyên trách, cơ quan điều phối ứng cứu sự cố an ninh mạng cấp trên.

đ) Tổng hợp, báo cáo và cập nhật diễn biến sự cố theo quy định.

3. Hoạt động của Đội ứng cứu sự cố an ninh mạng tỉnh khi tiếp nhận yêu cầu hỗ trợ điều phối hoặc thông báo sự cố:

a) Ghi nhận, tiếp nhận đúng quy định và phản hồi ngay cho tổ chức, cá nhân gửi thông báo hoặc yêu cầu hỗ trợ, điều phối.

b) Chủ trì, điều hành, phân công nhiệm vụ cho các thành viên Đội ứng cứu sự cố an ninh mạng tỉnh và các cơ quan, đơn vị liên quan triển khai xác minh và xử lý sự cố an ninh mạng.

c) Yêu cầu bên cung cấp dịch vụ viễn thông, Internet trên địa bàn phối hợp ngăn chặn nguồn tấn công, lọc lưu lượng độc hại.

d) Là đầu mối liên lạc, phối hợp với Trung tâm An ninh mạng quốc gia và các cơ quan Trung ương trong các trường hợp cần thiết.

Mục 5
BẢO VỆ BÍ MẬT NHÀ NƯỚC, DỮ LIỆU CÁ NHÂN

Điều 28. Bảo vệ bí mật nhà nước trên không gian mạng

1. Các cơ quan, đơn vị có xử lý thông tin bí mật nhà nước phải bố trí máy tính, máy in và các thiết bị ngoại vi được tách biệt hoàn toàn về mặt vật lý với mạng Internet và các mạng máy tính khác (trừ mạng LAN độc lập) để phục vụ riêng cho việc soạn thảo, lưu trữ, in ấn tài liệu bí mật nhà nước.

2. Không sử dụng máy tính, thiết bị đã dùng để soạn thảo, lưu giữ bí mật nhà nước để kết nối với mạng máy tính (trừ mạng LAN độc lập), mạng Internet, mạng viễn thông khi chưa hoàn thành việc chuyển mục đích sử dụng tài sản phần cứng; không sử dụng máy tính, thiết bị có lịch sử kết nối với mạng máy tính (trừ mạng LAN độc lập), mạng Internet, mạng viễn thông để soạn thảo, lưu giữ bí mật nhà nước.

3. Tài sản phần cứng, phần mềm phục vụ xử lý thông tin bí mật nhà nước phải được cơ quan chức năng kiểm tra, dán tem bảo đảm an ninh, an toàn thông tin trước khi đưa vào sử dụng (kể cả sau khi sửa chữa, bảo hành).

4. Tài sản phần cứng khi mang khỏi trụ sở của cơ quan, đơn vị phải được sự phê duyệt của cấp có thẩm quyền và thực hiện biện pháp bảo vệ đối với thông tin, tài liệu bí mật nhà nước lưu trữ trên tài sản phần cứng.

5. Các thiết bị lưu trữ di động (USB, Ổ cứng ngoài,...) dùng để sao chép, lưu trữ thông tin, tài liệu bí mật nhà nước phải được quản lý chặt chẽ, sử dụng riêng và áp dụng các biện pháp mã hóa để bảo vệ dữ liệu.

6. Việc truyền đưa thông tin thuộc bí mật nhà nước qua không gian mạng phải được mã hóa bằng sản phẩm mật mã của Ban Cơ yếu Chính phủ và tuân thủ tuyệt đối các quy định của pháp luật về cơ yếu, an ninh mạng, bảo vệ bí mật nhà nước.

Điều 29. Yêu cầu chung trong xử lý dữ liệu cá nhân

1. Việc xử lý dữ liệu cá nhân tại các cơ quan, đơn vị phải tuân thủ đầy đủ các nguyên tắc bảo vệ dữ liệu cá nhân quy định tại Điều 3 Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15.

2. Mọi hoạt động thu thập, xử lý dữ liệu cá nhân phải được sự đồng ý của chủ thể dữ liệu, trừ trường hợp pháp luật có quy định khác. Dữ liệu chỉ được xử lý đúng mục đích đã đăng ký hoặc thông báo.

3. Các cơ quan, đơn vị áp dụng các biện pháp quản lý và kỹ thuật phù hợp để bảo vệ dữ liệu cá nhân trong suốt quá trình xử lý, lưu trữ và hủy bỏ.

Điều 30. Quyền và nghĩa vụ của các bên liên quan trong bảo vệ dữ liệu cá nhân

1. Chủ thể dữ liệu là cán bộ, công chức, viên chức, người lao động và công dân có các quyền và nghĩa vụ theo quy định tại Điều 4 Luật số 91/2025/QH15.

2. Thủ trưởng cơ quan, đơn vị chịu trách nhiệm trực tiếp, toàn diện về việc bảo đảm an ninh dữ liệu cá nhân thuộc phạm vi quản lý của cơ quan, đơn vị mình.

3. Cán bộ, công chức, viên chức và người lao động được giao nhiệm vụ xử lý dữ liệu cá nhân có trách nhiệm bảo mật thông tin, không được tiết lộ, chia sẻ dữ liệu trái phép và phải chịu trách nhiệm nếu để xảy ra lộ, mất dữ liệu.

Điều 31. Trách nhiệm bảo vệ dữ liệu cá nhân của cơ quan, đơn vị

1. Các cơ quan, đơn vị là Bên Kiểm soát dữ liệu hoặc Bên Kiểm soát và xử lý dữ liệu cá nhân có trách nhiệm:

a) Phân công bộ phận hoặc nhân sự phụ trách bảo vệ dữ liệu cá nhân.

b) Xây dựng và ban hành nội dung quy định nội bộ về bảo vệ dữ liệu cá nhân.

c) Thực hiện đánh giá tác động xử lý dữ liệu cá nhân và lập hồ sơ gửi Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Bộ Công an theo quy định.

2. Khi phát hiện vi phạm hoặc sự cố về dữ liệu cá nhân, cơ quan, đơn vị phải tiến hành các biện pháp khắc phục ngay lập tức và thông báo cho cơ quan chuyên trách bảo vệ dữ liệu cá nhân chậm nhất 72 giờ kể từ khi phát hiện hành vi vi phạm hoặc sự cố dữ liệu cá nhân, trừ trường hợp pháp luật có quy định khác.

3. Áp dụng các biện pháp bảo vệ dữ liệu cá nhân trong hoạt động ứng dụng công nghệ thông tin, bao gồm: Quản lý quyền truy cập, ghi nhật ký hệ thống, mã hóa dữ liệu quan trọng và các biện pháp kỹ thuật khác theo hướng dẫn của cơ quan chức năng.

Chương III
TRÁCH NHIỆM BẢO ĐẢM AN NINH MẠNG

Điều 32. Trách nhiệm của Công an tỉnh

1. Tham mưu, quản lý nhà nước:

a) Chủ trì tham mưu, giúp Ủy ban nhân dân tỉnh thực hiện công tác quản lý nhà nước về an ninh mạng trên địa bàn tỉnh.

b) Xây dựng, trình Ủy ban nhân dân tỉnh ban hành và tổ chức thực hiện các chiến lược, chương trình, đề án, kế hoạch của tỉnh về bảo đảm an ninh mạng.

2. Thẩm định, thanh tra, kiểm tra, đánh giá:

a) Chủ trì thẩm định về an ninh mạng trong hồ sơ thiết kế hệ thống thông tin; thực hiện việc thẩm định hoặc cho ý kiến chuyên môn đối với hồ sơ đề xuất cấp độ hệ thống thông tin và phương án bảo đảm an ninh mạng theo thẩm quyền.

b) Chủ trì tổ chức kiểm tra, đánh giá an ninh mạng định kỳ và đột xuất đối với các hệ thống thông tin của tỉnh; yêu cầu các cơ quan, đơn vị khắc phục các lỗ hổng, điểm yếu bảo mật được phát hiện.

c) Chủ trì tổ chức kiểm tra, dán tem bảo đảm an ninh, an toàn thông tin đối với tài sản phần cứng, phần mềm phục vụ xử lý thông tin bí mật nhà nước.

3. Giám sát và cảnh báo:

a) Tổ chức quản lý, vận hành Trung tâm An ninh mạng tỉnh (nếu có); tổ chức giám sát tập trung, phân tích, cảnh báo sớm các nguy cơ, mối đe dọa an ninh mạng.

b) Chỉ đạo, hướng dẫn bảo đảm an ninh mạng cho hạ tầng kỹ thuật của các Trung tâm dữ liệu của tỉnh.

c) Chủ trì, phối hợp với các cơ quan chức năng xử lý thông tin vi phạm pháp luật trên không gian mạng.

d) Tổ chức triển khai kết nối, chia sẻ thông tin giám sát, cảnh báo với Trung tâm An ninh mạng quốc gia thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Bộ Công an.

4. Ứng cứu sự cố an ninh mạng:

a) Là đơn vị thường trực của Đội ứng cứu sự cố an ninh mạng tỉnh, giữ vai trò đầu mối tiếp nhận, điều phối các hoạt động ứng cứu sự cố an ninh mạng trên toàn tỉnh.

b) Tham mưu Ủy ban nhân dân tỉnh ban hành và tổ chức triển khai phương án ứng cứu sự cố an ninh mạng trên địa bàn tỉnh, kết nối với hệ thống phương án ứng cứu quốc gia.

5. Phòng, chống tội phạm và vi phạm pháp luật:

a) Chủ trì, phối hợp với các cơ quan chức năng trong công tác phòng, chống tấn công mạng, gián điệp mạng, khủng bố mạng, phòng, chống mã độc và các loại tội phạm sử dụng công nghệ cao. Kịp thời thông báo các phương thức, thủ đoạn mới của các loại tội phạm công nghệ cao.

b) Điều tra, xử lý các hành vi vi phạm pháp luật về an ninh mạng theo thẩm quyền.

c) Chủ trì triển khai các biện pháp bảo đảm an ninh mạng, bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân và bảo vệ trẻ em trên không gian mạng.

6. Hướng dẫn, bồi dưỡng nghiệp vụ và diễn tập:

a) Chỉ đạo, hướng dẫn nghiệp vụ về bảo đảm an ninh mạng; hỗ trợ giải quyết sự cố khi có yêu cầu. Hướng dẫn các cơ quan, đơn vị xây dựng quy chế

nội bộ và triển khai thực hiện việc bảo đảm an ninh mạng cho hệ thống thông tin theo quy định.

b) Hằng năm xây dựng kế hoạch, tổng hợp nhu cầu của các cơ quan, đơn vị để triển khai bồi dưỡng, tập huấn về an ninh mạng trong hoạt động ứng dụng công nghệ thông tin trên địa bàn tỉnh.

c) Chủ trì, phối hợp với các cơ quan liên quan tổ chức bồi dưỡng nghiệp vụ, tập huấn kỹ năng chuyên sâu về an ninh mạng cho lực lượng chuyên trách; xây dựng nội dung và triển khai các hoạt động tuyên truyền, phổ biến kiến thức, nâng cao nhận thức về an ninh mạng cho cán bộ, công chức, viên chức, người lao động và Nhân dân trên địa bàn tỉnh.

d) Chủ trì tổ chức các cuộc diễn tập ứng cứu sự cố an ninh mạng cấp tỉnh; tham gia các chương trình diễn tập quốc gia, quốc tế do Bộ Công an tổ chức.

Điều 33. Trách nhiệm của Sở Khoa học và Công nghệ

1. Chủ trì, tham mưu cho Ủy ban nhân dân tỉnh về chiến lược, chương trình, đề án, kế hoạch về ứng dụng công nghệ thông tin, chuyển đổi số, phát triển chính quyền số, kinh tế số và xã hội số trên địa bàn tỉnh, bảo đảm các yêu cầu về an ninh mạng được lồng ghép trong quá trình xây dựng.

2. Phối hợp với Công an tỉnh trong việc góp ý, đánh giá hoặc thẩm định các nội dung về công nghệ, hạ tầng số, hệ thống thông tin, nền tảng số thuộc các dự án đầu tư theo quy định của pháp luật; bảo đảm tuân thủ các yêu cầu về an ninh mạng.

3. Hướng dẫn, phổ biến quy định của pháp luật về chuyển đổi số, công nghệ số và phối hợp tuyên truyền, nâng cao nhận thức về an ninh mạng đối với các tổ chức, doanh nghiệp thuộc lĩnh vực quản lý của ngành theo quy định của pháp luật.

4. Cung cấp thông tin, ý kiến chuyên môn về kỹ thuật, công nghệ của các hệ thống thông tin, nền tảng số khi có yêu cầu của Công an tỉnh trong quá trình kiểm tra, đánh giá hoặc ứng cứu sự cố an ninh mạng.

5. Chủ trì hướng dẫn, đôn đốc các cơ quan, đơn vị triển khai, quản lý và khai thác hiệu quả hạ tầng số, nền tảng số dùng chung của tỉnh; thúc đẩy ứng dụng khoa học, công nghệ, đổi mới sáng tạo, trí tuệ nhân tạo (AI), dữ liệu số và chuyển đổi số, bảo đảm tuân thủ các yêu cầu về an toàn thông tin và an ninh mạng trong hoạt động của cơ quan nhà nước.

Điều 34. Trách nhiệm của Sở Tài chính

1. Chủ trì, phối hợp với các đơn vị liên quan tham mưu cấp có thẩm quyền bố trí kinh phí thực hiện các nhiệm vụ, đề án, dự án về bảo đảm an ninh mạng, an ninh thông tin, an ninh dữ liệu theo quy định của Luật Ngân sách nhà nước số 89/2025/QH15 và các văn bản hướng dẫn có liên quan.

2. Tổng hợp, tham mưu cấp có thẩm quyền về kế hoạch vốn trung hạn, hằng năm đối với các nhiệm vụ, đề án, dự án về bảo đảm an ninh mạng của các sở, ban, ngành, địa phương khi đủ điều kiện theo quy định.

Điều 35. Trách nhiệm của chủ quản hệ thống thông tin

1. Ủy ban nhân dân tỉnh có thể giao nhiệm vụ quản lý trực tiếp hệ thống thông tin thuộc lĩnh vực chuyên môn cho các cơ quan, đơn vị phụ trách và thực hiện đầy đủ trách nhiệm của chủ quản hệ thống thông tin.

2. Thủ trưởng các cơ quan, đơn vị là chủ quản hệ thống thông tin trực tiếp chỉ đạo và phụ trách công tác bảo đảm an ninh mạng; chịu trách nhiệm toàn diện trước Ủy ban nhân dân tỉnh và trước pháp luật về công tác bảo đảm an ninh mạng cho các hệ thống thông tin thuộc phạm vi quản lý của mình.

3. Phân công bộ phận hoặc cán bộ chuyên trách/phụ trách về an ninh mạng; bố trí đủ nguồn lực (nhân sự, kinh phí, trang thiết bị) để triển khai các nhiệm vụ bảo đảm an ninh mạng.

4. Trình cấp có thẩm quyền phê duyệt hồ sơ đề xuất cấp độ an ninh mạng của hệ thống thông tin; chỉ đạo xây dựng và ban hành phương án bảo đảm an ninh mạng tương ứng với cấp độ được duyệt và tổ chức triển khai thực hiện.

5. Ban hành và tổ chức thực hiện quy chế nội bộ về bảo đảm an ninh mạng tại cơ quan, đơn vị mình.

6. Tổ chức thực hiện việc kiểm tra, đánh giá, quản lý rủi ro an ninh mạng định kỳ theo quy định.

7. Phối hợp chặt chẽ với Công an tỉnh và các cơ quan, đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an ninh mạng.

8. Phối hợp, cung cấp thông tin và tạo điều kiện cho các cơ quan, đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố an ninh mạng kịp thời, nhanh chóng và đạt hiệu quả.

9. Các đơn vị có trách nhiệm bảo đảm an ninh mạng đối với hệ thống thông tin của mình; căn cứ quy mô, tính chất và cấp độ của hệ thống thông tin do đơn vị quản lý, thủ trưởng cơ quan, đơn vị có trách nhiệm phân công cán bộ, công chức, viên chức phụ trách công tác bảo đảm an ninh mạng; trường hợp hệ thống thông tin thuộc diện phải bố trí lực lượng bảo vệ an ninh mạng theo quy định của pháp luật, thực hiện theo quy định của Chính phủ và hướng dẫn của cơ quan có thẩm quyền.

Điều 36. Trách nhiệm của đơn vị vận hành hệ thống thông tin

1. Trách nhiệm của các cơ quan, đơn vị được cấp có thẩm quyền giao vận hành hệ thống thông tin:

a) Thực hiện xác định cấp độ hệ thống thông tin theo quy định tại Điều 14 Nghị định số 85/2016/NĐ-CP.

b) Thực hiện bảo đảm an ninh mạng hệ thống thông tin theo Quy chế này, các quy định của pháp luật và hướng dẫn, tiêu chuẩn, quy chuẩn an ninh mạng.

c) Định kỳ đánh giá hiệu quả của các biện pháp bảo đảm an ninh mạng báo cáo chủ quản hệ thống thông tin điều chỉnh nếu cần thiết.

d) Phối hợp, thực hiện theo yêu cầu của cơ quan chức năng trong công tác bảo đảm an ninh mạng.

đ) Kịp thời kích hoạt phương án ứng cứu sự cố và thông báo, phối hợp xử lý sự cố an ninh mạng với các cơ quan, đơn vị liên quan.

e) Định kỳ hoặc đột xuất báo cáo công tác thực thi bảo đảm an ninh mạng hệ thống thông tin theo yêu cầu của chủ quản hệ thống thông tin.

2. Trường hợp hệ thống thông tin có chủ quản đóng vai trò là đơn vị vận hành hệ thống thông tin thực hiện các quy định tại khoản 1 Điều này.

3. Trường hợp hệ thống thông tin thuê dịch vụ công nghệ thông tin (đã có hợp đồng thuê): Bên cung cấp dịch vụ đóng vai trò là đơn vị vận hành hệ thống thông tin, có trách nhiệm thực hiện các quy định tại khoản 1 Điều này; phối hợp chặt chẽ với đơn vị chủ quản hệ thống thông tin trong quá trình thực hiện.

Điều 37. Trách nhiệm của các Trung tâm dữ liệu của tỉnh

1. Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo Quy chế này.

2. Bảo đảm tiêu chuẩn, quy chuẩn kỹ thuật về trung tâm dữ liệu; phù hợp với quy hoạch hạ tầng thông tin và truyền thông; có giải pháp bảo đảm an ninh mạng để kiểm soát, phát hiện, ngăn chặn tấn công, đột nhập, phá hoại; bảo đảm mức độ sẵn sàng của hệ thống, thiết kế hệ thống với mức dự phòng nhằm sẵn sàng trong trường hợp mở rộng khi cần thiết.

3. Thường xuyên cập nhật các nguy cơ gây mất an ninh mạng cho các hệ thống thông tin đang cài đặt và vận hành tại các Trung tâm dữ liệu của tỉnh và thông báo cho các cơ quan, đơn vị liên quan biết để có biện pháp phòng ngừa, ngăn chặn, xử lý kịp thời.

Điều 38. Trách nhiệm của cán bộ, công chức, viên chức và người lao động

1. Trách nhiệm của cán bộ, công chức, viên chức và người lao động:

a) Chấp hành Quy chế này, quy chế nội bộ của cơ quan và các quy định của pháp luật về an ninh mạng. Chịu trách nhiệm bảo đảm an ninh mạng trong phạm vi trách nhiệm và quyền hạn được giao.

b) Cán bộ, công chức, viên chức và người lao động có trách nhiệm quản lý, bảo quản, bảo đảm an ninh mạng cho tài sản công nghệ thông tin được giao quản lý, sử dụng.

c) Khi phát hiện sự cố mất an ninh mạng phải thông báo ngay với cấp trên và bộ phận hoặc cán bộ chuyên trách/phụ trách về an ninh mạng của cơ quan, đơn vị để kịp thời ngăn chặn, xử lý.

d) Tham gia nghiêm túc các chương trình đào tạo, tập huấn, diễn tập về an ninh mạng do Ủy ban nhân dân tỉnh hoặc cơ quan chuyên trách về an ninh mạng tổ chức.

đ) Cán bộ, công chức, viên chức và người lao động trong các cơ quan, đơn vị có trách nhiệm bảo đảm an ninh mạng đối với hệ thống thông tin trong phạm vi xử lý công việc của mình theo quy định của Nhà nước, của ngành và các quy định liên quan.

2. Trách nhiệm của cán bộ chuyên trách/phụ trách về an ninh mạng: Ngoài các quy định tại khoản 1 Điều này, cán bộ chuyên trách/phụ trách về an ninh mạng có trách nhiệm:

a) Chủ trì tham mưu với thủ trưởng cơ quan, đơn vị thực hiện các quy định của Quy chế này và các quy định pháp luật có liên quan đến an ninh mạng.

b) Trực tiếp thiết lập hoặc tham mưu các biện pháp kỹ thuật bảo đảm an ninh mạng cho hạ tầng kỹ thuật, hệ thống thông tin trong cơ quan, đơn vị mình; hướng dẫn cán bộ, công chức, viên chức và người lao động trong cơ quan, đơn vị tuân thủ các biện pháp bảo đảm an ninh mạng trong hoạt động ứng dụng công nghệ thông tin.

c) Thực hiện việc giám sát, đánh giá, ghi nhật ký và báo cáo ngay Thủ trưởng cơ quan, đơn vị các sự cố mất an ninh mạng và mức độ nghiêm trọng của các sự cố đó.

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

Điều 39. Trách nhiệm của tổ chức, đơn vị, cá nhân liên quan

Các tổ chức, đơn vị, cá nhân liên quan đến sử dụng, khai thác các hệ thống thông tin của tỉnh hoặc có liên quan trực tiếp đến công tác bảo đảm an ninh mạng trên địa bàn tỉnh phải tuân thủ Quy chế này và các quy định hiện hành của pháp luật về an ninh mạng.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 40. Chế độ, nội dung báo cáo

Các cơ quan, đơn vị có trách nhiệm lập và gửi báo cáo cho Ủy ban nhân dân tỉnh (qua Công an tỉnh) về công tác an ninh mạng theo định kỳ và đột xuất:

1. Báo cáo định kỳ hằng năm về tình hình, kết quả thực hiện Quy chế này. Thời gian báo cáo trước ngày 15 tháng 12.

2. Báo cáo đột xuất: Báo cáo tình hình, kết quả triển khai phương án ứng cứu sự cố an ninh mạng trên địa bàn tỉnh; công tác khắc phục, xử lý các lỗ hổng, điểm yếu bảo mật, cảnh báo an ninh mạng và các báo cáo đột xuất khác theo yêu cầu của Công an tỉnh hoặc yêu cầu của Ủy ban nhân dân tỉnh.

3. Công an tỉnh chịu trách nhiệm tổng hợp báo cáo của các cơ quan, đơn vị, trình Ủy ban nhân dân tỉnh, gửi các cơ quan quản lý nhà nước về an ninh mạng.

Điều 41. Kinh phí thực hiện

Kinh phí bảo đảm an ninh mạng trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước trên địa bàn tỉnh Đắk Lắk được bố trí từ nguồn ngân sách nhà nước theo phân cấp ngân sách hiện hành và các nguồn kinh phí hợp pháp khác.

Điều 42. Trách nhiệm thi hành

1. Căn cứ Quy chế này, thủ trưởng các cơ quan, đơn vị và các tổ chức, đơn vị, cá nhân liên quan có trách nhiệm tổ chức triển khai thực hiện Quy chế này trong phạm vi quản lý của mình. Quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc phát sinh, các cơ quan, đơn vị phản ánh kịp thời về Công an tỉnh để tổng hợp, báo cáo Ủy ban nhân dân tỉnh xem xét sửa đổi, bổ sung.

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.