UBND TỈNH KHÁNH HÒA
BAN QUẢN LÝ KHU KINH TẾ VÀ KHU CÔNG NGHIỆP

Số: 36 /QĐ-KKTKCN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Khánh Hòa, ngày 24 tháng 02 năm 2026

QUYẾT ĐỊNH
Ban hành quy định, quy trình nội bộ về bảo đảm an ninh mạng, an toàn thông tin của Ban Quản lý Khu kinh tế và Khu công nghiệp tỉnh Khánh Hòa

TRƯỞNG BAN
BAN QUẢN LÝ KHU KINH TẾ VÀ KHU CÔNG NGHIỆP
TỈNH KHÁNH HÒA

Căn cứ Quyết định số 1570/QĐ-TTg ngày 21 tháng 7 năm 2025 của Thủ tướng Chính phủ về việc thành lập Ban Quản lý Khu kinh tế và Khu công nghiệp tỉnh Khánh Hòa;

Căn cứ Quyết định số 16/2025/QĐ-UBND ngày 22 tháng 8 năm 2025 của UBND tỉnh Khánh Hòa quy định chức năng, nhiệm vụ, quyền hạn của Ban Quản lý Khu kinh tế và Khu công nghiệp tỉnh Khánh Hòa;

Căn cứ Quyết định số 11/2026/QĐ-UBND ngày 31 tháng 01 năm 2026 của UBND tỉnh Khánh Hòa ban hành Quy chế bảo đảm an ninh mạng, an toàn thông tin trên địa bàn tỉnh Khánh Hòa;

Theo đề nghị của Chánh Văn phòng Ban Quản lý khu kinh tế và Khu công nghiệp tỉnh Khánh Hòa.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này quy định, quy trình nội bộ về bảo đảm an ninh mạng, an toàn thông tin của Ban Quản lý Khu kinh tế và Khu công nghiệp tỉnh Khánh Hòa.

Điều 2. Quyết định này có hiệu lực kể từ ngày ký.

Điều 3. Chánh Văn phòng, Trưởng các phòng, đơn vị trực thuộc Ban Quản lý Khu kinh tế và Khu công nghiệp tỉnh Khánh Hòa, tổ chức và cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3 (VBĐT);
- UBND tỉnh (để b/c – VBĐT);
- Công an tỉnh (để p/h – VBĐT);
- Sở KH&CN (để p/h – VBĐT);
- Lưu: VT, VP, HK.

TRƯỞNG BAN

BAN QUẢN LÝ KHU KINH TẾ VÀ KHU CÔNG NGHIỆP T. KHÁNH HÒA

Trần Minh Chiến

UBND TỈNH KHÁNH HÒA
BAN QUẢN LÝ KHU KINH TẾ VÀ KHU CÔNG NGHIỆP

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

QUY ĐỊNH, QUY TRÌNH NỘI BỘ
Về bảo đảm an ninh mạng, an toàn thông tin của Ban Quản lý Khu kinh tế và Khu công nghiệp tỉnh Khánh Hòa

Chương I
QUY ĐỊNH CHUNG

Điều 1. Mục đích

1. Thiết lập các quy định, quy trình nội bộ nhằm bảo đảm an ninh mạng, an toàn thông tin trong hoạt động quản lý, điều hành và cung cấp dịch vụ công của cơ quan.

2. Phòng ngừa, phát hiện, ngăn chặn và xử lý kịp thời các nguy cơ, sự cố mất an ninh mạng, an toàn thông tin.

Điều 2. Phạm vi và đối tượng áp dụng

1. Quy định này áp dụng đối với toàn bộ hệ thống thông tin, hạ tầng công nghệ thông tin, dữ liệu và trang thiết bị CNTT thuộc phạm vi quản lý của cơ quan.

2. Đối tượng áp dụng gồm: các phòng, đơn vị trực thuộc; công chức, viên chức, người lao động; tổ chức, cá nhân tham gia quản trị, vận hành, khai thác, sử dụng hệ thống thông tin của cơ quan.

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

1. Tuân thủ quy định của pháp luật và quy định của UBND tỉnh về an ninh mạng, an toàn thông tin.

2. Bảo đảm an ninh mạng, an toàn thông tin được thực hiện thường xuyên, liên tục từ khâu thiết kế, triển khai đến vận hành, khai thác hệ thống thông tin.

3. Xác định rõ trách nhiệm của người đứng đầu, bộ phận chuyên trách và người sử dụng.

Điều 4. Trách nhiệm chung

1. Người đứng đầu cơ quan chịu trách nhiệm toàn diện về công tác bảo đảm an ninh mạng, an toàn thông tin.

2. Văn phòng Ban (Bộ phận CNTT) là đầu mối tham mưu, tổ chức triển khai các biện pháp kỹ thuật, giám sát, ứng cứu sự cố.

3. Người sử dụng hệ thống thông tin có trách nhiệm tuân thủ nghiêm các quy định tại văn bản này.

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

Điều 5. Quản lý 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 6. Thuê dịch vụ công nghệ thông tin

1. Khi ký kết hợp đồng thuê dịch vụ công nghệ thông tin, cơ quan phải xác định rõ phạm vi, trách nhiệm, quyền hạn và nghĩa vụ của các bên về bảo đảm an toàn thông tin. Trong hợp đồng phải bao gồm các điều khoản về việc xử lý vi phạm quy định bảo đảm an toàn thông tin và trách nhiệm bồi thường thiệt hại do hành vi vi phạm của bên cung cấp dịch vụ gây ra.

2. Trách nhiệm của Phòng, đơn vị thuộc Ban trong quá trình sử dụng dịch vụ công nghệ thông tin:

a) Quản lý thông tin, dữ liệu phát sinh từ dịch vụ đó, không để bên cung cấp dịch vụ truy cập, sử dụng thông tin, dữ liệu thuộc phạm vi Nhà nước quản lý.

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

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

3. Trách nhiệm của Phòng, đơn vị khi phát hiện bên cung cấp dịch vụ có dấu hiệu vi phạm quy định bảo đảm an toàn thông tin phải báo cáo, xin chỉ đạo của Lãnh đạo Ban để thực hiện các nội dung sau:

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 Phòng, đơn vị khi kết thúc sử dụng dịch vụ phải báo cáo, xin chỉ đạo của Lãnh đạo Ban để thực hiện:

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

Hệ thống thông tin của cơ quan phải được phân loại, xác định và áp dụng biện pháp bảo đảm an toàn theo cấp độ quy định tại 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.

CHƯƠNG III
BẢO ĐẢM AN TOÀN DỮ LIỆU

Điều 8. Phân loại dữ liệu

Dữ liệu được phân loại gồm: dữ liệu thông thường; dữ liệu nhạy cảm; dữ liệu thuộc bí mật nhà nước và được quản lý theo quy định pháp luật.

1. Dữ liệu công khai (Dữ liệu thông thường)

- Nội dung: Bao gồm các văn bản quy phạm pháp luật, thủ tục hành chính, tin tức hoạt động, các thông báo phổ biến đã được phê duyệt công bố rộng rãi trên cổng thông tin điện tử hoặc các phương tiện thông tin đại chúng.

- Quy định quản lý:

+ Được phép chia sẻ rộng rãi mà không cần kiểm soát quyền truy cập.

+ Phải đảm bảo tính toàn vẹn (không bị sửa đổi trái phép) để tránh sai lệch thông tin chính thống.

2. Dữ liệu dùng riêng (Dữ liệu nhạy cảm)

- Nội dung: Bao gồm các thông tin lưu hành nội bộ, hồ sơ nhân sự, dữ liệu cá nhân của người dùng, dữ liệu của tổ chức/doanh nghiệp trong khu kinh tế, các báo cáo tài chính nội bộ, mã nguồn phần mềm và tài liệu thiết kế hệ thống.

- Quy định quản lý:

+ Kiểm soát truy cập: Chỉ những cá nhân có chức trách, nhiệm vụ phù hợp với vị trí công tác mới được quyền tiếp cận.

+ Lưu trữ: Phải được lưu trữ trên các hệ thống có xác thực và mã hóa khi truyền đưa qua mạng.

+ Chia sẻ: Khi chia sẻ cho bên thứ ba (như đơn vị cung cấp dịch vụ CNTT) phải có thỏa thuận bảo mật bằng văn bản và giới hạn quyền truy cập tối thiểu.

3. Dữ liệu bí mật nhà nước

- Nội dung: Các thông tin, tài liệu thuộc danh mục bí mật nhà nước (độ: Tuyệt mật, Tối mật, Mật) theo quy định của pháp luật về bảo vệ bí mật nhà nước.

- Quy định quản lý:

+ Tách biệt hoàn toàn: Nghiêm cấm lưu trữ, soạn thảo, trao đổi dữ liệu bí mật nhà nước trên các máy tính, thiết bị kết nối mạng Internet hoặc mạng nội bộ chưa được kiểm điểm, phê duyệt về an ninh.

+ Quy trình xử lý: Việc sao chép, vận chuyển, lưu trữ và tiêu hủy phải tuân thủ nghiêm ngặt theo quy định hiện hành của Luật Bảo vệ bí mật nhà nước.

+ Thiết bị chuyên dụng: Chỉ sử dụng các thiết bị đã qua kiểm tra, đánh giá an ninh mạng để xử lý loại dữ liệu này.

Điều 9. Lưu trữ, sao lưu và khôi phục dữ liệu

Dữ liệu phải được sao lưu định kỳ theo mô hình phù hợp, bảo đảm khả năng khôi phục khi xảy ra sự cố.

Thực hiện kiểm tra, thử nghiệm khôi phục dữ liệu định kỳ.

Điều 10. Chia sẻ, trao đổi và cung cấp dữ liệu

Việc chia sẻ, cung cấp dữ liệu phải đúng thẩm quyền, đúng mục đích và bảo đảm an toàn, bảo mật thông tin.

Điều 11. Bảo vệ dữ liệu cá nhân và dữ liệu của tổ chức, doanh nghiệp

Thực hiện các biện pháp kỹ thuật và quản lý để bảo vệ dữ liệu cá nhân, dữ liệu của tổ chức, doanh nghiệp theo quy định của pháp luật.

CHƯƠNG IV
BẢO ĐẢM AN TOÀN THIẾT BỊ VÀ NGƯỜI DÙNG ĐẦU CUỐI

Điều 12. Quản lý thiết bị 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 13. Quản lý tài khoản, mật khẩu và quyền truy cập

1. Quản lý tài khoản người dùng:

- Tài khoản chỉ được cấp phát dựa trên văn bản phê duyệt của cấp có thẩm quyền. Phải thực hiện thu hồi hoặc vô hiệu hóa tài khoản ngay lập tức (không quá 24 giờ) khi nhân sự nghỉ việc, thay đổi vị trí công tác hoặc hết hạn hợp đồng.

- Mỗi cá nhân chỉ được sử dụng duy nhất một tài khoản định danh riêng biệt. Nghiêm cấm việc chia sẻ tài khoản dùng chung cho các mục đích tác nghiệp thông thường.

- Định kỳ ít nhất 06 tháng/lần, bộ phận quản trị hệ thống phải thực hiện rà soát danh sách tài khoản để loại bỏ các tài khoản không còn sử dụng hoặc sai mục đích.

2. Chính sách mật khẩu:

Mật khẩu phải đảm bảo độ phức tạp và được quản lý theo các tiêu chuẩn sau:

- Độ dài và ký tự: Tối thiểu 08 ký tự, bao gồm ít nhất 03 trong 4 loại ký tự: chữ hoa, chữ thường, số và ký tự đặc biệt.

- Thời hạn sử dụng: Yêu cầu thay đổi mật khẩu định kỳ (ví dụ: tối đa 90 ngày). Không được sử dụng lại mật khẩu của 03 lần gần nhất.

- Bảo mật mật khẩu: Không ghi chép mật khẩu ra giấy, không lưu trữ dưới dạng văn bản không mã hóa (clear-text) trên máy tính hoặc các thiết bị di động.

- Xác thực đa yếu tố (MFA): Bắt buộc áp dụng xác thực 2 lớp (MFA/2FA) đối với các tài khoản có quyền quản trị hoặc tài khoản truy cập vào hệ thống lõi từ mạng bên ngoài.

3. Phân quyền truy cập:

Việc phân quyền phải tuân thủ nghiêm ngặt nguyên tắc trong bảo mật:

- Người dùng chỉ được cấp quyền truy cập vừa đủ để hoàn thành nhiệm vụ được giao. Không cấp thừa quyền so với vị trí công tác.

- Người dùng chỉ có quyền tiếp cận thông tin khi thông tin đó thực sự cần thiết cho công việc hiện tại.

- Phân định rõ chức năng, nhiệm vụ giữa người quản trị hệ thống, người quản trị an toàn thông tin và người vận hành để tránh xung đột lợi ích và lạm dụng quyền hạn.

Điều 14. Trách nhiệm của người sử dụng

Người sử dụng có trách nhiệm bảo vệ tài khoản, thiết bị được giao; không thực hiện các hành vi làm mất an toàn thông tin.

CHƯƠNG V
GIÁM SÁT, PHÁT HIỆN VÀ ỨNG CỨU SỰ CỐ

Điều 15. Giám sát và tiếp nhận cảnh báo

Bộ phận CNTT thực hiện giám sát, tiếp nhận cảnh báo và kịp thời xử lý các nguy cơ mất an toàn thông tin.

Điều 16. Quy trình xử lý sự cố

1. Nguyên tắc ứng cứu xử lý sự cố:

a) Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả;

b) Phối hợp chặt chẽ, tuân thủ quy định của pháp luật về điều phối ứng cứu sự cố an toàn thông tin;

c) Ứng cứu xử lý sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin;

d) Việc xử lý sự cố an toàn thông tin phải bảo đảm quyền và lợi ích hợp pháp của cơ quan, đơn vị, cá nhân, bảo mật thông tin cá nhân, thông tin riêng của cơ quan, đơn vị khi tham gia các hoạt động ứng cứu xử lý sự cố.

2. Phân nhóm sự cố an toàn thông tin:

a) Sự cố do bị tấn công mạng

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

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

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

d) Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin: Hoạt động ứng cứu sự cố an toàn thông tin mạng huy động các nguồn lực nằm ngoài phạm vi của đơn vị vận hành hệ thống thông tin để đối phó với các sự cố quy định tại khoản 1 Điều này.

3. Phân loại mức độ nghiêm trọng sự cố:

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

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

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

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

đ) 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, đơn vị và người dân, doanh nghiệp, đe dọa trật tự an toàn xã hội.

4. Quy trình phối hợp ứng cứu xử lý sự cố:

a) Bước 1: Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc thẩm quyền cơ quan, đơn vị trực tiếp quản lý thì thực hiện tiếp Bước 2. Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Khoa học và Công nghệ quản lý thì thực hiện tiếp Bước 3;

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

c) Bước 3: Báo sự cố đến Sở Khoa học và Công nghệ theo mẫu số 01 kèm theo Quy chế;

d) Bước 4: Phối hợp với Khoa học và Công nghệ và các cơ quan, đơn vị, tổ chức có liên quan để tiến hành khắc phục sự cố và thực hiện tiếp Bước 5;

đ) Bước 5: Lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố theo mẫu số 02 kèm theo Quy chế này. Lãnh đạo cơ quan, đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại, báo cáo bằng văn bản cho cơ quan cấp trên trực tiếp quản lý và Sở Khoa học và Công nghệ.

5. Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của cơ quan, đơn vị: Lãnh đạo cơ quan, đơn vị phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và Sở Khoa học và Công nghệ để được hướng dẫn, hỗ trợ.

6. 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 toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng;

b) Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng 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, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống;

d) Tổ chức diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của Lãnh đạo.

Điều 17. Phối hợp với cơ quan chuyên trách

Đối với sự cố nghiêm trọng, thực hiện báo cáo và phối hợp xử lý với Công an tỉnh, Sở Khoa học và Công nghệ theo quy định.

CHƯƠNG VI
TỔ CHỨC THỰC HIỆN

Điều 18. Đào tạo, tuyên truyền và diễn tập

Hằng năm tổ chức đào tạo, tuyên truyền nâng cao nhận thức và diễn tập ứng cứu sự cố an ninh mạng.

Điều 19. Kiểm tra, đánh giá

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

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

c) Kiểm tra công tác giám sát an toàn thông tin và ứng phó khi xảy ra sự cố an toàn thông tin;

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

Điều 20. Khen thưởng và xử lý vi phạm

Tổ chức, cá nhân có thành tích được khen thưởng; trường hợp vi phạm bị xử lý theo quy định pháp luật.

Điều 21. Hiệu lực thi hành

Quy định này có hiệu lực kể từ ngày ký ban hành và được áp dụng thống nhất trong toàn cơ quan.