UBND TỈNH QUẢNG TRỊ **VĂN PHÒNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 105 /QĐ-VP	*Quảng Trị, ngày22 tháng12 năm 2025*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số của Văn phòng UBND tỉnh Quảng Trị

CHÁNH VĂN PHÒNG UBND TỈNH QUẢNG TRỊ

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

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

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

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

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

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

Căn cứ Quyết định số 02/2025/QĐ-UBND ngày 31 tháng 7 năm 2025 của Ủy ban nhân dân tỉnh Quảng Trị ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Văn phòng Ủy ban nhân dân tỉnh Quảng Trị;

Theo đề nghị của Giám đốc Trung tâm Điều hành thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin mạng trong hoạt động phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số của Văn phòng UBND tỉnh Quảng Trị.

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

Điều 3. Giám đốc Trung tâm Điều hành thông tin, Trưởng các phòng, ban, trung tâm thuộc Văn phòng và các tổ chức, cá nhân liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- CT, các PCT UBND tỉnh (b/c);
- Công an tỉnh (PA05);
- Sở Khoa học và Công nghệ;
- Lãnh đạo Văn phòng UBND tỉnh;
- BCĐ về PTKH, CN, ĐMST, CĐS và ĐA 06 VP UBND tỉnh;
- Lưu: VT, ĐHTT.

CHÁNH VĂN PHÒNG

CỘNG HÒA X.H.C.N VIỆT NAM
VĂN PHÒNG ỦY BAN NHÂN DÂN
TỈNH QUẢNG TRỊ

Nguyễn Hoài Nam

UBND TỈNH QUẢNG TRỊ
VĂN PHÒNG

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

QUY CHẾ

Bảo đảm an toàn thông tin mạng trong hoạt động phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số của Văn phòng UBND tỉnh Quảng Trị

(Kèm theo Quyết định số 105 /QĐ-VP ngày 22 /12/2025 của Văn phòng UBND tỉnh Quảng Trị)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về việc bảo đảm an toàn thông tin mạng trong hoạt động phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số của các phòng, ban, trung tâm thuộc Văn phòng UBND tỉnh Quảng Trị (sau đây gọi tắt là Văn phòng).

Điều 2. Đối tượng áp dụng

1. Các phòng, ban, trung tâm thuộc Văn phòng.

2. Cá nhân là công chức, viên chức, người lao động của các phòng, ban, trung tâm thuộc Văn phòng và các cá nhân khác liên quan.

Điều 3. Giải thích từ ngữ

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

1. Các khái niệm *"an toàn thông tin mạng", "mạng", "hệ thống thông tin", "chủ quản hệ thống thông tin", "xâm phạm an toàn thông tin mạng", "sự cố an toàn thông tin mạng", "rủi ro an toàn thông tin mạng", "phần mềm độc hại ", "xung đột thông tin", "thông tin cá nhân", "xử lý thông tin cá nhân*" được định nghĩa theo quy định tại các khoản 1, 2, 3, 5, 6, 7, 8, 11, 14, 15 và 17 Điều 3 Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015.

2. Các khái niệm *"tội phạm mạng", "tấn công mạng", "khủng bố mạng", "gián điệp mạng"* được định nghĩa theo quy định tại các khoản 7, 8, 9 và 10 Điều 2 Luật An ninh mạng ngày 12 tháng 6 năm 2018.

3. *Nguy cơ mất an toàn thông tin mạng* là những nhân tố bên trong hoặc bên ngoài có khả năng ảnh hưởng tới trạng thái an toàn thông tin mạng.

4. *Trung tâm tích hợp dữ liệu* là nơi chứa các thiết bị phần cứng, thiết bị mạng, phần mềm, hệ thống lưu trữ tập trung, các thiết bị bảo mật thông tin, các thiết bị lưu điện phục vụ công việc của Văn phòng.

Điều 4. Mục đích, nguyên tắc bảo đảm an toàn thông tin mạng

1. Việc áp dụng Quy chế này nhằm phòng ngừa, ngăn chặn, xử lý và giảm các nguy cơ gây mất an toàn thông tin mạng và bảo đảm an ninh thông tin trong hoạt động phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số của Văn phòng.

2. Hoạt động phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số của Văn phòng phải tuân thủ nguyên tắc bảo đảm an toàn thông tin mạng được quy định tại Điều 4 Luật An toàn thông tin mạng và Điều 41 Nghị định số 64/2007/NĐ-CP.

Điều 5. Các hành vi bị cấm

1. Các hành vi bị nghiêm cấm về an toàn, an ninh thông tin mạng quy định tại Điều 7 Luật An toàn thông tin mạng và Điều 8 Luật An ninh mạng.

2. Tự ý lắp đặt các thiết bị thu, phát sóng Wifi (Access Point) vào mạng máy tính của Văn phòng khi chưa được phê duyệt của Lãnh đạo Văn phòng.

3. Tự ý đăng tải, sao chép, chia sẻ, truyền đưa, tải về hoặc sử dụng dưới bất kỳ hình thức nào các dữ liệu, tài liệu, số liệu nội bộ, văn bản chưa được công khai hoặc thông tin thuộc danh mục bí mật của cơ quan, đơn vị lên mạng Internet, mạng xã hội, thư điện tử công cộng hay phương tiện truyền thông đại chúng khác.

4. Cài đặt, sử dụng phần mềm, ứng dụng, hoặc thiết bị không rõ nguồn gốc, không được kiểm duyệt an toàn, có khả năng gây rò rỉ thông tin hoặc xâm nhập trái phép vào hệ thống mạng.

5. Cố ý can thiệp, thay đổi cấu hình, phá hoại, hoặc làm gián đoạn hoạt động của hệ thống mạng, máy chủ, thiết bị lưu trữ, hoặc phần mềm dùng chung của cơ quan.

Chương II
ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 6. Yêu cầu chung về quản lý an toàn thông tin mạng

1. Đối với các phòng, ban, trung tâm thuộc Văn phòng:

a) Phân loại thông tin do mình sở hữu theo thuộc tính bí mật để có biện pháp bảo vệ phù hợp theo quy định của pháp luật về bảo vệ bí mật nhà nước. Khi sử dụng thông tin đã phân loại và chưa phân loại trong hoạt động thuộc lĩnh vực của mình phải xây dựng quy định, thủ tục để xử lý thông tin; xác định nội dung và phương pháp ghi truy nhập được phép vào thông tin đã được phân loại.

b) Áp dụng các biện pháp quản lý và kỹ thuật phù hợp để ngăn chặn mất an toàn thông tin mạng; phối hợp, cung cấp thông tin liên quan đến an toàn tài nguyên viễn thông theo yêu cầu của cơ quan nhà nước có thẩm quyền.

c) Tổ chức các biện pháp bảo vệ hệ thống thông tin, ngăn chặn xung đột

thông tin trên mạng thuộc quyền quản lý và phối hợp chặt chẽ với cơ quan nghiệp vụ theo quy định của pháp luật để triển khai các biện pháp ngăn chặn xung đột thông tin trên mạng khi vượt quá thẩm quyền, khả năng.

d) Áp dụng các biện pháp quản lý và kỹ thuật phù hợp để ngăn chặn thông tin phá hoại xuất phát từ hệ thống thông tin của mình. Hợp tác với các cơ quan chức năng xác định nguồn, đẩy lùi, khắc phục hậu quả.

đ) Xây dựng và công bố công khai biện pháp xử lý, bảo vệ thông tin cá nhân của đơn vị mình. Khi xử lý thông tin cá nhân phải có trách nhiệm bảo đảm an toàn thông tin mạng đối với thông tin do mình xử lý.

e) Thường xuyên tuyên truyền, phổ biến, nâng cao nhận thức của công chức, viên chức, người lao động về trách nhiệm bảo đảm an toàn thông tin mạng. Khi tiếp nhận nhân sự mới phải quán triệt các quy định, quy chế, quy trình, thủ tục an toàn thông tin mạng. Khi nhân sự chuyển công tác, nghỉ việc, nghỉ theo chế độ phải phối hợp với Trung tâm Điều hành thông tin tổ chức bàn giao, thu hồi tài khoản, quyền truy nhập và tất cả tài sản liên quan tới các hệ thống thông tin của cơ quan.

f) Trung tâm Điều hành thông tin thường xuyên theo dõi, kiểm tra các lỗ hổng bảo mật và quản lý kết nối, truy cập khi sử dụng thiết bị đầu cuối từ xa; cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống đối với cán bộ đã nghỉ việc; cấu hình tối ưu, tăng cường bảo mật (cứng hóa) cho máy tính người sử dụng.

2. Đối với cá nhân công chức, viên chức, người lao động:

a) Thường xuyên cập nhật và nghiêm túc chấp hành quy định, quy chế, quy trình, thủ tục an toàn thông tin mạng của cơ quan và thực hiện các hướng dẫn, khuyến cáo của Trung tâm Điều hành thông tin.

b) Tự bảo vệ thông tin cá nhân của mình và tuân thủ quy định của pháp luật về cung cấp thông tin cá nhân khi sử dụng dịch vụ trên mạng, đồng thời có trách nhiệm bảo đảm an toàn thông tin mạng đối với thông tin do mình xử lý.

c) Khi tham gia quản lý, vận hành mạng máy tính của cơ quan phải nghiêm chỉnh chấp hành chế độ bảo mật, an toàn, an ninh thông tin mạng đồng thời chịu trách nhiệm đối với các thông tin mà mình cung cấp.

d) Tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp các thiết bị trên máy tính làm ảnh hưởng đến an toàn thông tin mạng; không được vào các trang thông tin điện tử không rõ về nội dung; không tải và cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn; không truy cập vào các liên kết lạ không rõ về nội dung; không cung cấp thông tin không trung thực để công bố trên mạng; sử dụng mạng để truy cập vào các mạng máy tính khi chưa được phép; không đưa các thông tin, tài liệu chứa bí mật nhà nước lên hệ thống máy tính có kết nối mạng Internet.

đ) Phải sử dụng thư điện tử công vụ và các công cụ trao đổi thông tin, dữ liệu

do các cơ quan nhà nước hoặc tổ chức có thẩm quyền cung cấp, cho phép sử dụng trong trao đổi thông tin, dữ liệu phục vụ công việc; không sử dụng các trang mạng xã hội, dịch vụ thư điện tử, các phần mềm chat, công cụ tiện ích điện tử công cộng để trao đổi thông tin quan trọng liên quan đến công việc chuyên môn của cơ quan.

e) Khi phát hiện nguy cơ mất an toàn thông tin mạng hoặc dấu hiệu sự cố an toàn thông tin mạng phải báo cáo kịp thời với cấp trên và Trung tâm Điều hành thông tin để xem xét, tham mưu, tổ chức ngăn chặn, xử lý, khắc phục.

f) Luôn quét virus trước khi đọc hoặc sao chép dữ liệu từ các thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB....

g) Không sử dụng các máy tính thuộc sở hữu cá nhân (máy xách tay) hoặc những thiết bị lưu trữ di động cá nhân vào các công việc của Văn phòng. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.

h) Các thiết bị đầu cuối khi kết nối phải được quản lý và cập nhật thông tin (tên, chủng loại, địa chỉ MAC, địa chỉ IP).

Điều 7. Quản lý đăng nhập, khai thác, sử dụng hệ thống thông tin

1. Thiết lập mật mã truy nhập và chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng cho tất cả máy chủ, máy tính cá nhân.

2. Bảo vệ bí mật thông tin tài khoản của cá nhân hoặc tài khoản của cơ quan khi được phân công quản lý, đồng thời phải thay đổi ngay mật khẩu tài khoản khi mới được cấp và tự chịu trách nhiệm trong việc quản lý, sử dụng và bảo vệ mật khẩu của tài khoản. Không được cho người khác sử dụng tài khoản của cá nhân hoặc của cơ quan.

3. Thiết lập mật khẩu đăng nhập, truy nhập khai thác, sử dụng hệ thống thông tin có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như !, @, #, $, %) và phải thay đổi ít nhất 03 tháng/lần. Không đặt chế độ tự động ghi nhớ mật khẩu đăng nhập, truy nhập khai thác, sử dụng hệ thống thông tin trên các trình duyệt của máy tính trong mọi trường hợp.

4. Cán bộ quản trị phải vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ nghỉ hoặc thay đổi công tác.

Điều 8. Quản lý Trung tâm tích hợp dữ liệu

1. Hệ thống phần mềm, phần cứng, các thiết bị bảo mật, thiết bị lưu trữ dữ liệu, lưu điện đặt tại Trung tâm tích hợp dữ liệu phải được chạy vận hành thử nghiệm và kiểm tra an toàn thông tin trước khi đưa vào sử dụng; phải có tài liệu hướng dẫn sử dụng, quy trình vận hành và thủ tục vận hành, quy trình quản lý sự cố liên quan đến an toàn thông tin; phải có các văn bản xác định vai trò, trách nhiệm của từng cá nhân trong quá trình vận hành và sử dụng.

2. Quản lý nhật ký quá trình vận hành hệ thống phần cứng, phần mềm, các thiết bị bảo mật, thiết bị lưu trữ dữ liệu, lưu điện đặt tại Trung tâm tích hợp dữ

liệu:

a) Trung tâm Điều hành thông tin phải tổ chức thực hiện việc ghi nhật ký trên các thiết bị phần cứng, 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 và lưu giữ. Các bản ghi nhật ký này phải được bảo vệ an toàn nhằm sử dụng để phục vụ công tác kiểm tra, phân tích khi cần thiết.

b) Các sự kiện tối thiểu 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 nhập hệ thống.

c) Trung tâm Điều hành thông tin thường xuyên theo dõi bản ghi nhật ký của các hệ thống đặt tại Trung tâm tích hợp dữ liệu và các sự kiện khác có liên quan để đánh giá, báo cáo các rủi ro an toàn thông tin mạng và mức độ nghiêm trọng các rủi ro đó.

d) Máy chủ phải được thiết lập chính sách xác thực và kiểm soát truy cập. Các hệ thống thông tin cần có phương án giới hạn số lần đăng nhập, tự động khóa tài khoản khi liên tục đăng nhập sai vượt quá số lần quy định. Tổ chức theo dõi, giám sát tất cả các phương pháp đăng nhập từ xa, nhất là các trường hợp đăng nhập vào hệ thống với mục đích quản trị.

e) Kiểm tra, giám sát các hoạt động liên quan đến các nơi lưu trữ mật khẩu và cảnh báo khi có những hành động bất thường.

3. Quản lý vận hành đối với phòng máy Trung tâm tích hợp dữ liệu:

a) Các thiết bị kết nối mạng, thiết bị bảo mật quan trọng như bộ chuyển mạch trung tâm, thiết bị định tuyến, thiết bị tường lửa, hệ thống máy chủ, hệ thống lưu trữ SAN, NAS, thiết bị cảm biến, giám sát an toàn thông tin, thiết bị bảo mật, phòng chống tấn công mạng phải đặt trong Trung tâm tích hợp dữ liệu được thiết lập, thực hiện các cơ chế, biện pháp kiểm soát truy nhập, kết nối vật lý, bảo vệ, theo dõi phát hiện xâm nhập phù hợp.

b) Trung tâm tích hợp dữ liệu phải được trang bị hệ thống lưu điện, hệ thống phát điện dự phòng, hệ thống làm mát, điều hòa không khí, độ ẩm, hệ thống cảnh báo nguồn điện, hệ thống chống sét lan truyền, hệ thống cảnh báo cháy, hệ thống cảm biến nhiệt độ, hệ thống chữa cháy tự động bằng khí, thiết bị phòng cháy, chữa cháy khẩn cấp bảo đảm tiêu chuẩn, quy chuẩn kỹ thuật và tương xứng với quy mô, tính chất, yêu cầu phục vụ.

c) Trung tâm Điều hành thông tin trực tiếp quản lý Trung tâm tích hợp dữ liệu có trách nhiệm xây dựng nội quy hoặc hướng dẫn làm việc và cử cán bộ thường xuyên giám sát thiết bị, hạ tầng tại Trung tâm tích hợp dữ liệu.

4. Quản lý an toàn mạng:

a) Hệ thống mạng phải được thiết kế thống nhất, được quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý và bảo đảm an toàn và bảo mật.

b) Hệ thống mạng nội bộ (LAN) phải được bảo vệ bằng tường lửa (có thể tích hợp tường lửa trên modem hoặc router) và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng.

c) Mạng không dây (WIFI), cần thiết lập các thông số an toàn và định kỳ thay đổi mật khẩu truy cập để tăng cường công tác bảo mật. Hệ thống mạng không dây phải được bảo vệ bởi mật khẩu an toàn.

5. Quản lý an toàn dữ liệu:

a) Có cơ chế sao lưu dữ liệu dự phòng, lưu trữ dữ liệu tại nơi an toàn đồng thời thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố an toàn thông tin mạng xảy ra. Dữ liệu trên máy chủ được sao lưu thông qua hệ thống sao lưu dữ liệu.

b) Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống theo yêu cầu.

c) Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của cán bộ kỹ thuật và phải được phê duyệt từ lãnh đạo.

Điều 9. Phòng, chống phần mềm độc hại

1. Tất cả máy chủ, máy trạm khuyến cáo được trang bị phần mềm phòng, chống phần mềm độc hại có bản quyền và đã được cơ quan chức năng khuyến cáo sử dụng. Phần mềm phòng, chống phần mềm độc hại phải được thiết lập chế độ tự động cập nhật và chế độ tự động quét phần mềm độc hại khi sao chép, mở các tệp tin.

2. Hệ điều hành, phần mềm cài đặt trên máy chủ, máy trạm phải được cập nhật vá lỗ hổng bảo mật thường xuyên, kịp thời theo khuyến cáo của nhà phát triển phần mềm.

3. Cá nhân không được tự ý gỡ bỏ các phần mềm phòng, chống phần mềm độc hại trên máy tính khi chưa có sự đồng ý của người có thẩm quyền.

4. Tất cả các máy tính phải được cấu hình vô hiệu hóa tính năng tự động thực thi (autoplay) các tệp tin trên các thiết bị lưu trữ di động kết nối vào.

5. Máy tính xách tay, thiết bị di động (máy tính bảng, điện thoại thông minh, thiết bị có phần mềm hệ điều hành) trước khi kết nối vào mạng nội bộ (LAN) của cơ quan phải bảo đảm đã được cài đặt phần mềm phòng, chống phần mềm độc hại và đã được kiểm duyệt về các phần mềm độc hại.

6. Máy chủ chỉ được dùng để cài đặt các phần mềm, dịch vụ dùng chung của cơ quan; không cài đặt phần mềm không rõ nguồn gốc, phần mềm phục vụ mục đích cá nhân và không phục vụ công việc.

7. Khi kết nối từ xa vào máy chủ để quản trị, phải sử dụng phương thức kết nối có mã hóa. Khuyến khích sử dụng mạng diện rộng của tỉnh để truy nhập, khai thác các hệ thống thông tin dùng chung của tỉnh.

8. Tất cả các tệp tin, thư mục phải được quét phần mềm độc hại trước khi sao chép, sử dụng.

9. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy trạm như: Hoạt động chậm bất thường, có cảnh báo từ phần mềm phòng chống phần mềm độc hại, tình trạng này lặp đi lặp lại nhiều lần, ở các vị trí khác nhau, nhất là có dấu hiệu bị thay đổi, mất dữ liệu, người sử dụng phải tắt máy, ngắt kết nối từ máy tính đến mạng nội bộ (LAN), mạng diện rộng (WAN), mạng Internet và báo cáo, thông báo trực tiếp cho Trung tâm Điều hành thông tin để tiến hành kiểm tra, xử lý.

Điều 10. Sao lưu dữ liệu dự phòng

1. Trung tâm Điều hành thông tin có trách nhiệm:

a) Thực hiện quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn.

b) Xác định danh sách các hệ thống phần cứng, phần mềm, cơ sở dữ liệu cần được sao lưu, có phân loại theo thời gian lưu trữ, phương pháp sao lưu và thời gian phục hồi dữ liệu; ban hành và thực hiện quy trình sao lưu dự phòng và phục hồi dữ liệu, phần mềm.

c) Tổ chức lưu trữ dữ liệu sao lưu ở nơi an toàn, không cùng phân vùng lưu trữ các ứng dụng và thường xuyên kiểm tra, bảo đảm sẵn sàng cho việc sử dụng khi cần thiết.

d) Có cơ chế sao lưu dữ liệu dự phòng, đồng thời thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố an toàn thông tin mạng xảy ra.

e) Tiến hành cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ.

f) Sử dụng mật mã để bảo đảm an toàn và bảo mật dữ liệu trong lưu trữ.

g) Quản lý chặt chẽ các thiết bị lưu trữ dữ liệu, nghiêm cấm việc di chuyển, thay đổi vị trí khi chưa được phép.

h) Quản lý, phân quyền truy cập phần mềm ứng dụng và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của cán bộ, công chức, viên chức và phải được phê duyệt từ lãnh đạo.

i) Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: Tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

2. Các phòng, ban, trung tâm và cán bộ, công chức, viên chức tại Văn phòng có trách nhiệm:

a) Lập kế hoạch và thực hiện sao lưu dữ liệu dự phòng định kỳ đối với các dữ liệu quan trọng, tối thiểu mỗi tháng một lần; trường hợp cần thiết phải áp dụng kỹ thuật mã hóa, thiết lập mật mã, ứng dụng ký số chứng thực.

b) Việc sao lưu dữ liệu dự phòng phải bảo đảm tính đầy đủ, toàn vẹn, và tin cậy. Sau khi sao lưu phải lưu trữ bản sao lưu bằng thiết bị lưu trữ ngoài phù hợp, bảo đảm tính bảo mật và sẵn sàng cho việc phục hồi dữ liệu khi cần thiết.

Điều 11. Ứng cứu sự cố an toàn thông tin mạng

1. Phân loại mức độ sự cố an toàn thông tin mạng:

a) Sự cố mức độ thấp (thông thường): Sự cố gây ảnh hưởng đến 01 (một) hoặc một vài cá nhân đơn lẻ và không làm gián đoạn hay đình trệ hoạt động chính của Văn phòng như: Máy tính cá nhân bị nhiễm phần mềm độc hại hoặc hư hỏng phần cứng; phần mềm hệ điều hành, các phần mềm ứng dụng, tiện ích cài đặt trên máy tính cá nhân phát sinh lỗi.

b) Sự cố mức độ trung bình: Sự cố ảnh hưởng đến một nhóm lớn người khai thác, sử dụng nhưng vẫn chưa gây gián đoạn hoạt động chính của Văn phòng như: Hệ thống mạng của 01 (một) phòng, ban, trung tâm thuộc Văn phòng bị ngưng hoạt động; phần mềm độc hại lây nhiễm tất cả các máy tính trạm trong 01 (một) phòng, ban , trung tâm.

c) Sự cố mức độ cao: Sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến một trong các hoạt động chính của Văn phòng như: Ứng dụng quản lý văn bản và điều hành, một cửa điện tử, Cổng Thông tin điện tử, Phần mềm Công báo... của toàn Văn phòng bị ngưng hoạt động; một số thiết bị công nghệ thông tin quan trọng (bộ chuyển mạch trung tâm, thiết bị định tuyến…) bị hư hỏng.

d) Sự cố có tính chất nghiêm trọng: Sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính tại Văn phòng như toàn bộ hệ thống thiết bị công nghệ thông tin ngừng hoạt động; hệ thống Cổng/trang thông tin điện tử thành phần, các hệ thống phần mềm do Văn phòng UBND tỉnh quản lý, điều hành bị tin tặc (hacker) tấn công, xâm nhập, thay đổi nội dung; hoặc sự cố có một hoặc nhiều tính chất sau: Có khả năng xảy ra trên diện rộng, lan nhanh; có khả năng phá hoại hệ thống mạng máy tính, lấy cắp dữ liệu,...

2. Khi có nguy cơ mất an toàn thông tin mạng hoặc sự cố an toàn thông tin mạng xảy ra ở mức độ trung bình thì Văn phòng chỉ đạo bộ phận phụ trách công nghệ thông tin phối hợp với đơn vị, cá nhân bị ảnh hưởng tự xử lý, khắc phục

hoặc liên hệ với đơn vị cung cấp sản phẩm, dịch vụ viễn thông, Internet, đơn vị triển khai ứng dụng phần mềm để được tư vấn, hỗ trợ ngăn chặn, xử lý, khắc phục.

3. Khi có nguy cơ hoặc sự cố an toàn thông tin mạng xảy ra ở mức độ cao trở lên, xét thấy không có khả năng tự xử lý được thì Trung tâm Điều hành thông tin báo cáo Lãnh đạo Văn phòng và thông báo cho Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh hoặc Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam để tổ chức điều phối, hỗ trợ ứng cứu.

Điều 12. Đưa hệ thống thông tin vào sử dụng, và kết thúc vận hành hệ thống thông tin

1. Đối với việc thiết kế hệ thống thông tin mới:

a) Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin.

b) Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.

c) Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.

d) Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.

e) Đối với việc phát triển phần mềm, hệ thống thông tin thuê khoán phải có điều khoản hợp đồng và các cam kết đối với bên thuê khoán khi thực hiện các nội dung liên quan đến việc phát triển phần mềm thuê khoán.

2. Đối với việc thử nghiệm, nghiệm thu hệ thống thông tin:

a) Đơn vị triển khai có trách nhiệm xây dựng kế hoạch và nội dung thử nghiệm hệ thống, trình cấp có thẩm quyền xem xét, phê duyệt trước khi tổ chức thực hiện việc thử nghiệm và nghiệm thu hệ thống.

b) Hệ thống thông tin phải được tổ chức kiểm thử đầy đủ theo đúng nội dung, kế hoạch đã được phê duyệt trước khi đưa vào vận hành, khai thác và sử dụng chính thức.

c) Việc thử nghiệm và nghiệm thu hệ thống do bộ phận kỹ thuật chuyên môn thực hiện theo quy định.

3. Kết thúc vận hành hệ thống thông tin:

a) Khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống phải được bộ phận chuyên trách an toàn thông tin thực hiện kiểm tra, đánh giá bảo đảm an toàn thông tin.

b) Quá trình xử lý thông tin trên hệ thống phải được thực hiện khi thay đổi mục đích sử dụng hoặc gỡ bỏ theo phương án kỹ thuật được phê duyệt.

Chương III
TỔ CHỨC THỰC HIỆN

Điều 13. Tổ chức thực hiện

1. Ban Chỉ đạo về phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số và Đề án 06 Văn phòng UBND tỉnh: Theo dõi, chỉ đạo các phòng, ban, trung tâm thực hiện Quy chế này.

2. Trung tâm Điều hành thông tin:

a) Thực hiện các trách nhiệm được giao; hướng dẫn triển khai Quy chế theo các quy định hiện hành.

c) Định kỳ, xây dựng kế hoạch, báo cáo về an toàn, an ninh thông tin mạng của Văn phòng theo yêu cầu của cơ quan quản lý nhà nước về an toàn thông tin; thường xuyên kiểm tra tính phù hợp để thực hiện rà soát, cập nhật, bổ sung.

3. Các phòng, ban, trung tâm thuộc Văn phòng:

a) Trưởng các phòng, ban, trung tâm có trách nhiệm: Phổ biến tới từng công chức, viên chức, người lao động; thường xuyên kiểm tra việc thực hiện Quy chế này tại phòng, ban, trung tâm; chịu trách nhiệm trước pháp luật và Lãnh đạo Văn phòng về các vi phạm, thất thoát thông tin, dữ liệu mật thuộc phạm vi quản lý của phòng, ban, trung tâm do không tổ chức, chỉ đạo, kiểm tra công chức, viên chức, người lao động thuộc quyền quản lý thực hiện đúng quy định.

b) Công chức, viên chức, người lao động thuộc đối tượng áp dụng của Quy chế có trách nhiệm: Tuân thủ Quy chế; thông báo các vấn đề bất thường liên quan tới an toàn thông tin cho Lãnh đạo Văn phòng, bộ phận chuyên trách về an toàn thông tin mạng của cơ quan; chịu trách nhiệm trước pháp luật và Lãnh đạo Văn phòng về các vi phạm, thất thoát dữ liệu mật do không tuân thủ Quy chế.

Trong quá trình triển khai thực hiện Quy chế, nếu có vấn đề phát sinh, vướng mắc, các phòng, ban, trung tâm phản hồi (qua Trung tâm Điều hành thông tin) để tổng hợp, báo cáo Chánh Văn phòng xem xét, sửa đổi, bổ sung./.