ỦY BAN NHÂN DÂN TỈNH QUẢNG NINH	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 36/2023/QĐ-UBND	*Quảng Ninh, ngày 25 tháng 12 năm 2023*

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn thông tin mạng cho các Hệ thống thông tin cấp độ 3 tại Trung tâm tích hợp dữ liệu tỉnh

ỦY BAN NHÂN DÂN TỈNH QUẢNG NINH

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

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

Căn cứ Luật Công nghệ thông tin ngày 29/6/2006; Luật An toàn thông tin mạng ngày 19/11/2015; Luật An ninh mạng ngày 12/6/2018; Luật Bảo vệ bí mật nhà nước ngày 15/11/2018;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 142/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng;

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

Căn cứ Chỉ thị số 02/CT-TTg ngày 26/4/2022 của Thủ tướng Chính phủ về phát triển Chính phủ điện tử hướng tới Chính phủ số, thúc đẩy chuyển đổi số quốc gia;

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

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

Căn cứ Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của 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 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ 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;

Theo đề nghị của Sở Thông tin và Truyền thông tại Tờ trình số 1008/TTr-STTTT ngày 13/12/2023; ý kiến thẩm định của Sở Tư pháp tại Báo cáo thẩm định số 303/BC-STP ngày 29/9/2023 và ý kiến tham gia của thành viên UBND tỉnh.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn thông tin mạng cho các Hệ thống thông tin cấp độ 3 tại Trung tâm tích hợp dữ liệu tỉnh.

Điều 2. Quyết định này có hiệu lực từ ngày 15 tháng 01 năm 2024.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh; Thủ trưởng các sở, ban, ngành; Chủ tịch Ủy ban nhân dân các huyện, thị xã, thành phố; Thủ trưởng các cơ quan, đơn vị có liên quan chịu trách nhiệm thi hành Quyết định này./.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH
(Đã ký)

Cao Tường Huy

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

QUY CHẾ

Bảo đảm an toàn thông tin mạng
cho các Hệ thống thông tin cấp độ 3 tại Trung tâm tích hợp dữ liệu tỉnh

(Ban hành kèm theo Quyết định số 36/2023/QĐ-UBND ngày 25/12/2023 của UBND tỉnh Quảng Ninh)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh:

Quy chế này quy định các chính sách quản lý và các biện pháp nhằm bảo đảm an toàn thông tin cho các Hệ thống thông tin tại Trung tâm tích hợp dữ liệu tỉnh bao gồm:

a) Phạm vi quản lý về hạ tầng kỹ thuật của Trung tâm tích hợp dữ liệu tỉnh;

b) Các ứng dụng, dịch vụ hệ thống thông tin tại Trung tâm tích hợp dữ liệu tỉnh cung cấp;

c) Nguồn nhân lực bảo đảm an toàn thông tin.

2. Đối tượng áp dụng

a) Các sở, ban, ngành, đơn vị thuộc UBND tỉnh Quảng Ninh có hệ thống thông tin đặt tại Trung tâm tích hợp dữ liệu tỉnh;

b) Cơ quan, tổ chức, cá nhân có kết nối, sử dụng hệ thống thông tin tại Trung tâm tích hợp dữ liệu tỉnh;

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ quản lý, vận hành, duy trì, phát triển và bảo đảm an toàn thông tin mạng phục vụ hoạt động của các Hệ thống thông tin cấp độ 3 tại Trung tâm tích hợp dữ liệu tỉnh.

Điều 2. Giải thích từ ngữ

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

1. "Mạng", "An toàn thông tin mạng", "Hệ thống thông tin", "thông tin cá nhân", "Sự cố an toàn thông tin mạng", "Rủi ro an toàn thông tin mạng", "Phần mềm độc hại" được hiểu theo Điều 3, Chương I, Luật An toàn thông tin mạng 2015.

2. "Tấn công mạng", "An ninh mạng", "Tội phạm mạng", "Gián điệp mạng" được hiểu theo Điều 2, Chương I, Luật An ninh mạng 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.

Điều 3. Mục tiêu, nguyên tắc bảo đảm an toàn thông tin mạng

1. Mục tiêu bảo đảm an toàn thông tin mạng: Bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin cho các Hệ thống thông tin cấp độ 3 tại Trung tâm THDL tỉnh.

2. Nguyên tắc

a) Cơ quan, tổ chức, cá nhân thuộc đối tượng áp dụng Quy chế này có trách nhiệm bảo đảm an toàn thông tin và hệ thống thông tin trong phạm vi xử lý công việc của mình theo quy định của pháp luật, hướng dẫn của cơ quan, đơn vị có thẩm quyền và các quy định tại Quy chế này.

b) Bảo đảm an toàn thông tin mạng là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục trong quá trình:

Thu thập, tạo lập, xử lý, truyền tải, lưu trữ và sử dụng thông tin, dữ liệu.

Thiết kế, thiết lập và vận hành, nâng cấp, hủy bỏ hệ thống thông tin.

c) Việc bảo đảm an toàn các Hệ thống thông tin cấp độ 3 tại Trung tâm THDL tỉnh được thực hiện một cách tổng thể, đồng bộ, tập trung trong việc đầu tư các giải pháp bảo vệ, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp.

Điều 4. Những hành vi nghiêm cấm

Các hành vi bị nghiêm cấm được quy định tại Điều 7 Luật An toàn thông tin mạng 2015 và Điều 8 Luật An ninh mạng 2018, cụ thể:

1. Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật.

2. Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy nhập hệ thống thông tin của người sử dụng.

3. Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin.

4. Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

5. Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.

6. Xâm nhập trái pháp luật bí mật mật mã và thông tin đã mã hóa hợp pháp của cơ quan, tổ chức, cá nhân; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc.

7. Hành vi quy định tại khoản 1 Điều 18 của Luật An ninh mạng số 24/2018/QH14.

8. Tổ chức, hoạt động, câu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam.

9. Xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc.

10. Thông tin sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác;

11. Hoạt động mại dâm, tệ nạn xã hội, mua bán người; đăng tải thông tin dâm ô, đồi trụy, tội ác; phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng.

12. Xúi giục, lôi kéo, kích động người khác phạm tội.

13. Thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng; gây sự cố, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại hệ thống thông tin quan trọng về an ninh quốc gia.

14. Sản xuất, đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; phát tán chương trình tin học gây hại cho hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; xâm nhập trái phép vào mạng viễn thông, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của người khác.

15. Chống lại hoặc cản trở hoạt động của lực lượng bảo vệ an ninh mạng; tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng biện pháp bảo vệ an ninh mạng.

16. Lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc để trục lợi.

17. Hành vi khác vi phạm quy định của Luật An ninh mạng 2018.

Điều 5. Phối hợp với những cơ quan/tổ chức có thẩm quyền

1. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin:

Sở Thông tin và Truyền thông là đầu mối liên hệ đồng thời là đơn vị chuyên trách về an toàn thông tin có trách nhiệm xây dựng và thực thi chính sách an toàn thông tin; phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin phục vụ việc bảo đảm an toàn thông tin mạng cho các Hệ thống thông tin và hạ tầng kỹ thuật tại Trung tâm tích hợp dữ liệu tỉnh; tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin của các Hệ thống thông tin cấp độ 3 tại Trung tâm tích hợp dữ liệu tỉnh.

2. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin tại Trung tâm tích hợp dữ liệu tỉnh:

Trung tâm Công nghệ thông tin và Truyền thông. Điện thoại: 0203.3533.338 Email: qnict@quangninh.gov.vn. Tùy theo mức độ sự cố, phối hợp với các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng.

3. Các sở, ban, ngành, đơn vị, UBND các huyện, thị xã, thành phố: Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của các cơ quan, tổ chức có thẩm quyền; tham gia các chiến dịch An toàn thông tin; diễn tập ứng cứu an toàn thông tin do Bộ Thông tin và Truyền thông, tỉnh Quảng Ninh tổ chức.

Điều 6. Bảo đảm nguồn nhân lực

1. Tuyển dụng

a) Công chức, viên chức được tuyển dụng làm nhiệm vụ về an toàn thông tin có trình độ, chuyên môn về lĩnh vực công nghệ thông tin, an toàn thông tin bảo đảm phù hợp với yêu cầu vị trí việc làm và tiêu chuẩn chức danh nghề nghiệp viên chức theo quy định.

b) Thực hiện tuyển dụng công chức, viên chức bảo đảm đúng quy trình, thủ tục pháp luật hiện hành và phân cấp tuyển dụng công chức, viên chức của tỉnh.

c) Thực hiện đánh giá năng lực của công chức, viên chức phù hợp với vị trí tuyển dụng.

2. Trong quá trình làm việc

a) Công chức, viên chức thực hiện nhiệm vụ tại vị trí an toàn thông tin, cán bộ, công chức, viên chức khai thác sử dụng các Hệ thống thông tin tại Trung tâm THDL tỉnh phải tuân thủ và thực hiện nghiêm túc nội quy, quy chế bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống.

b) Hàng năm tổ chức quán triệt, phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng.

c) Hàng năm tổ chức đào tạo về an toàn thông tin cho người dùng trong hệ thống.

3. Chấm dứt hoặc thay đổi công việc

a) Công chức, viên chức chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức.

b) Thực hiện đúng quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi công chức, viên chức thôi việc, nghỉ hưu.

c) Lập biên bản cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc, nghỉ hưu, chuyển công tác.

Chương II

BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ THIẾT KẾ, XÂY DỰNG HỆ THỐNG

Điều 7. Thiết kế an toàn hệ thống thông tin

1. Đối với hệ thống phải thông qua đặt hàng để thiết kế, không có sẵn dịch vụ công nghệ thông tin trên thị trường.

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 bảo đảm an toàn thông tin theo cấp độ.

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

đ) 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.

2. Đối với dịch vụ công nghệ thông tin có sẵn trên thị trường

a) Có biên bản, hợp đồng và các cam kết đối với bên thuê dịch vụ các nội dung liên quan đến việc đơn vị cung cấp dịch vụ là đơn vị vận hành hệ thống.

b) Có cam kết của đơn vị cung cấp dịch vụ về bảo đảm tính bí mật và bản quyền của dịch vụ.

c) Yêu cầu đơn vị cung cấp dịch vụ cung cấp các tài khoản quản trị, mã nguồn hệ thống. Hỗ trợ chỉnh sửa khi có yêu cầu.

Điều 8. Phát triển phần mềm thuê khoán

Đối với việc thuê dịch vụ phát triển phần mềm theo hình thức thuê khoán cần phải:

1. Có biên bản, hợp đồng và các cam kết đối với bên thuê dịch vụ các nội dung liên quan đến việc phát triển phần mềm thực hiện theo hình thức thuê dịch vụ.

2. Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm.

3. Kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.

4. Kiểm tra, đánh giá an toàn thông tin trước khi đưa vào sử dụng.

5. Phát triển phần mềm theo khung phát triển phần mềm an toàn theo hướng dẫn của Cục An toàn thông tin - Bộ Thông tin và Truyền thông tại Công văn số 166/CATTT-ATHTTT ngày 10/12/2022 v/v Ban hành hướng dẫn "Khung phát triển phần mềm an toàn (phiên bản 1.0)".

Điều 9. Vận hành thử/kiểm thử và nghiệm thu hệ thống

1. Thực hiện vận hành thử/kiểm thử và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng.

2. Có nội dung, kế hoạch thực hiện vận hành thử/kiểm thử theo quy định.

3. Có bộ phận có trách nhiệm thực hiện tham gia vận hành thử/kiểm thử và nghiệm thu hệ thống.

4. Có đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình vận hành thử/kiểm thử và nghiệm thu hệ thống.

5. Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng.

Chương III

BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ VẬN HÀNH HỆ THỐNG

Điều 10. Quản lý an toàn mạng

Thực hiện theo quy định tại khoản 5, khoản 8, Điều 8 (Quy định về an toàn hoạt động) tại Quyết định số 26/2018/QĐ-UBND ngày 20/9/2018 của Ủy ban nhân dân tỉnh Quảng Ninh về việc ban hành Quy chế quản lý, khai thác và vận hành Trung tâm tích hợp dữ liệu tỉnh Quảng Ninh. Đồng thời thực hiện các quy định cụ thể như sau:

1. Quản lý, vận hành hoạt động bình thường của hệ thống:

a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn.

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

c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm.

d) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp.

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

e) Các bản quyền phần mềm cần được thống kê, quản lý thời gian phục vụ cho việc gia hạn và duy trì việc gia hạn bản quyền, dịch vụ bản quyền hàng năm.

g) Triển khai hệ thống phát hiện phòng chống xâm nhập giữa các vùng mạng quan trọng.

h) Sử dụng thêm các phương pháp xác thực đa nhân tố đối với các thiết bị mạng quan trọng.

i) Triển khai phương án cảnh báo thời gian thực trực tiếp đến người quản trị hệ thống thông qua hệ thống giám sát khi phát hiện sự cố trên các thiết bị mạng.

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

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

b) Triển khai phương án dự phòng nóng cho các thiết bị mạng chính bảo đảm khả năng vận hành liên tục của hệ thống; năng lực của thiết bị dự phòng phải đáp ứng theo quy mô hoạt động của hệ thống.

c) Triển khai hệ thống/phương tiện lưu trữ nhật ký độc lập và phù hợp với hoạt động của các thiết bị mạng. Dữ liệu nhật ký phải được lưu tối thiểu 06 tháng.

d) Triển khai hệ thống/phương tiện chống thất thoát dữ liệu trong hệ thống.

3. Truy cập và quản lý cấu hình hệ thống:

a) Cán bộ quản lý, nhân viên vận hành truy cập, khai thác thông tin tại hệ thống theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài.

b) Cán bộ quản lý, nhân viên vận hành có trách nhiệm theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho cán bộ quản lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.

c) Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác.

d) Quy trình kết nối thiết bị đầu cuối của người sử dụng vào hệ thống mạng; truy nhập và quản lý cấu hình hệ thống; cấu hình tối ưu, tăng cường bảo mật cho thiết bị

mạng, bảo mật (cứng hóa) trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.

Điều 11. Quản lý an toàn máy chủ và ứng dụng

Thực hiện theo quy định tại khoản 9, Điều 8 (Quy định về an toàn hoạt động) tại Quyết định số 26/2018/QĐ-UBND ngày 20/9/2018 của Ủy ban nhân dân tỉnh Quảng Ninh về việc ban hành Quy chế quản lý, khai thác và vận hành Trung tâm tích hợp dữ liệu tỉnh Quảng Ninh. Đồng thời thực hiện các quy định cụ thể như sau:

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

a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn.

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

c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm.

d) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp.

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

e) Các bản quyền phần mềm cần được thống kê, quản lý thời gian hạn phục vụ cho việc gia hạn.

2. Truy cập mạng của máy chủ:

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

3. Truy cập và quản trị máy chủ và ứng dụng:

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

b) Cấp quyền quản lý truy cập của người sử dụng trên máy chủ cài đặt hệ điều hành.

c) Toàn bộ máy chủ và thiết bị công nghệ thông tin không phải máy tính ngoại trừ các hệ thống bắt buộc phải có giao tiếp với Internet (các hệ thống phục vụ truy cập Internet; cung cấp giao diện ra Internet của trang tin điện tử; phục vụ cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công) không được kết nối Internet.

d) Sử dụng cơ chế xác thực đa nhân tố khi truy cập vào các máy chủ trong hệ thống, các tài khoản quản trị của ứng dụng; có cơ chế yêu cầu người sử dụng thay đổi thông tin xác thực định kỳ.

đ) Kiểm tra tính toàn vẹn của các tệp tin hệ thống và tính toàn vẹn của các quyền đã được cấp trên các tài khoản hệ thống.

e) Sử dụng cơ chế mã hóa thông tin xác thực của người sử dụng/bên sử dụng trước khi gửi đến ứng dụng qua môi trường mạng.

g) Xác thực thông tin, nguồn gửi khi trao đổi thông tin trong quá trình quản trị ứng dụng (không phải là thông tin, dữ liệu công khai) qua môi trường mạng.

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

5. Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng dụng.

6. Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống.

7. Cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác.

Điều 12. Quản lý an toàn dữ liệu

Thực hiện theo quy định tại khoản 10 Điều 8 (Quy định về an toàn hoạt động) tại Quyết định số 26/2018/QĐ-UBND ngày 20/9/2018 của Ủy ban nhân dân tỉnh Quảng Ninh về việc ban hành Quy chế quản lý, khai thác và vận hành Trung tâm tích hợp dữ liệu tỉnh Quảng Ninh.

Thực hiện quy định cụ thể về "Yêu cầu an toàn đối với phương pháp mã hóa" như sau:

1. Đơn vị phải xây dựng và áp dụng quy định sử dụng các phương thức mã hóa thích hợp theo các chuẩn quốc gia hoặc quốc tế đã được công nhận để bảo vệ thông tin.

2. Phải có biện pháp quản lý khóa mã hóa thích hợp để hỗ trợ việc sử dụng các kỹ thuật mã hóa.

Điều 13. Quản lý an toàn thiết bị đầu cuối

Thực hiện theo quy định tại khoản 11, Điều 8 (Quy định về an toàn hoạt động) tại Quyết định số 26/2018/QĐ-UBND ngày 20/9/2018 của Ủy ban nhân dân tỉnh Quảng Ninh về việc ban hành Quy chế quản lý, khai thác và vận hành Trung tâm tích hợp dữ liệu tỉnh Quảng Ninh.

Điều 14. Quản lý phòng chống phần mềm độc hại

Thực hiện theo quy định tại khoản 12, Điều 8 (Quy định về an toàn hoạt động) tại Quyết định số 26/2018/QĐ-UBND ngày 20/9/2018 của Ủy ban nhân dân tỉnh Quảng Ninh về việc ban hành Quy chế quản lý, khai thác và vận hành Trung tâm tích hợp dữ liệu tỉnh Quảng Ninh.

Điều 15. Quản lý giám sát an toàn hệ thống thông tin

Thực hiện theo quy định tại khoản 13, Điều 8 (Quy định về an toàn hoạt động) tại Quyết định số 26/2018/QĐ-UBND ngày 20/9/2018 của Ủy ban nhân dân tỉnh Quảng Ninh về việc ban hành Quy chế quản lý, khai thác và vận hành Trung tâm tích hợp dữ liệu tỉnh Quảng Ninh.

Điều 16. Quản lý điểm yếu an toàn thông tin

Thực hiện theo quy định tại khoản 14, Điều 8 (Quy định về an toàn hoạt động) tại Quyết định số 26/2018/QĐ-UBND ngày 20/9/2018 của Ủy ban nhân dân tỉnh Quảng Ninh về việc ban hành Quy chế quản lý, khai thác và vận hành Trung tâm tích hợp dữ liệu tỉnh Quảng Ninh.

Thực hiện theo quy định tại Điều 9 (Quy định về xử lý sự cố) tại Quyết định số 26/2018/QĐ-UBND ngày 20/9/2018 của UBND tỉnh Quảng Ninh về việc ban hành Quy chế quản lý, khai thác và vận hành Trung tâm tích hợp dữ liệu tỉnh Quảng Ninh. Đồng thời thực hiện các quy định cụ thể như sau:

1. Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; 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.

2. Có phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng.

3. Có Kế hoạch ứng phó sự cố an toàn thông tin mạng.

4. Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin.

5. Có Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường.

6. Có Quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng.

7. Có cơ chế 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.

8. Định kỳ tổ chức diễn tập phương án xử lý sự cố an toàn thông tin.

Điều 18. Quản lý an toàn người sử dụng đầu cuối

Thực hiện theo quy định tại khoản 15, Điều 8 (Quy định về an toàn hoạt động) tại Quyết định số 26/2018/QĐ-UBND ngày 20/9/2018 của Ủy ban nhân dân tỉnh Quảng Ninh về việc ban hành Quy chế quản lý, khai thác và vận hành Trung tâm tích hợp dữ liệu tỉnh Quảng Ninh.

Điều 19. Quản lý rủi ro an toàn thông tin

1. Phương pháp đánh giá rủi ro

2. Đánh giá rủi ro

a) Xác định rủi ro

Xác định bối cảnh nội bộ và bên ngoài đối với phạm vi áp dụng;

Xác định mối đe dọa liên quan đến các tài sản thông tin;

Xác định các mối đe dọa liên quan đến các hệ thống thông tin quan trọng, các hệ thống thông tin trọng yếu;

Xác định các điểm yếu của tài sản.

b) Phân tích rủi ro

Đánh giá mức độ hiện tại đang áp dụng;

Xác định khả năng xảy ra và tác động;

So sánh tiêu chí chấp nhận rủi ro.

3. Xử lý rủi ro.

a) Biện pháp xử lý rủi ro;

b) Xác định lại giá trị rủi ro;

c) So sánh tiêu chí chấp nhận;

d) Biện pháp xử lý rủi ro theo quy trình khắc phục.

4. Giám sát và đánh giá.

Điều 20. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

1. Quy định hủy bỏ các thông tin/dữ liệu bảo mật.

2. Quy định về xử lý và hủy bỏ phương tiện lưu trữ điện tử:

a) Thiết bị công nghệ thông tin có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng phải được cán bộ chuyên trách về công nghệ thông tin kiểm tra, sửa chữa, khắc phục. Phải có biện pháp kiểm tra, giám sát bảo đảm không để lọt lộ thông tin hay lây nhiễm mã độc đối với máy tính mang ra bên ngoài sửa chữa, bảo hành.

b) Trước khi tiến hành thanh lý/loại bỏ thiết bị công nghệ thông tin cũ, phải áp dụng các biện pháp kỹ thuật xóa bỏ hoàn toàn dữ liệu người dùng đã tạo ra, bảo đảm không thể phục hồi.

3. Quy định về xử lý thông tin trên các phương tiện và thiết bị công nghệ thông tin: Máy tính cá nhân (PC), máy tính xách tay, máy chủ, các thiết bị mạng, phương tiện lưu trữ như CD/DVD, thẻ nhớ, ổ cứng…

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 21. Trách nhiệm của Sở Thông tin và Truyền thông

1. Chủ trì, hướng dẫn các cơ quan, tổ chức triển khai thực hiện Quy chế này và các quy định có liên quan đến an toàn thông tin mạng.

2. Thành lập hoặc chỉ định đơn vị chuyên trách về an toàn thông tin trong tổ chức.

3. Xây dựng kế hoạch kiểm tra, đánh giá hàng năm tình hình an toàn thông tin tại các cơ quan, đơn vị.

4. Hướng dẫn các cơ quan, đơn vị triển khai lập, trình phê duyệt hồ sơ cấp độ an toàn hệ thống thông tin của đơn vị; thẩm định hồ sơ cấp độ an toàn thông tin các Hệ thống thông tin của các cơ quan đơn vị.

5. Là đầu mối đại diện cho UBND tỉnh tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của cấp trên.

6. Tổng hợp, báo cáo Ủy ban nhân dân tỉnh, Bộ Thông tin và Truyền thông về an toàn thông tin trên địa bàn tỉnh.

Điều 22. Trách nhiệm của các đơn vị, tổ chức, cá nhân có hệ thống, thiết bị đặt tại Trung tâm Tích hợp dữ liệu

1. Cử đầu mối phối hợp, liên hệ khi làm việc tại Trung tâm tích hợp dữ liệu tỉnh.

2. Có trách nhiệm xây dựng Quy chế đảm bảo an toàn thông tin cho từng hệ thống, thiết bị của mình theo Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016; Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ Thông tin và Truyền thông trước khi đặt tại Trung tâm tích hợp dữ liệu tỉnh.

3. Thực hiện nghiêm túc quy chế làm việc tại Trung tâm tích hợp dữ liệu tỉnh và theo sự hướng dẫn của cán bộ quản lý, vận hành Trung tâm tích hợp dữ liệu tỉnh.

4. Sử dụng đúng tài khoản được cấp để truy cập từ xa. Thực hiện nghiêm túc Điều 4 Quy chế này.

5. Các đơn vị có kế hoạch đặt thiết bị tại Trung tâm tích hợp dữ liệu tỉnh cần phải đảm bảo an toàn thông tin cấp độ cho các hệ thống phù hợp. Các thiết bị trước khi lắp đặt phải được kiểm tra và có tem chứng nhận đảm bảo an toàn thông tin của Bộ Công an.

6. Các đơn vị có kế hoạch đặt thiết bị, hệ thống tại Trung tâm tích hợp dữ liệu cần có hồ sơ cấp độ an toàn thông tin cho hệ thống do Ủy ban nhân dân tỉnh quyết định cấp độ hệ thống.

7. Các đơn vị, tổ chức, cá nhân đặt thiết bị, hệ thống tại Trung tâm tích hợp dữ liệu chịu hoàn toàn trách nhiệm khi có sự cố về mất an toàn, an ninh thông tin do hệ thống của mình gây ra.

Điều 23. Trách nhiệm của cơ quan, đơn vị, địa phương

1. Thực hiện trách nhiệm của cơ quan, tổ chức quản lý Hệ thống thông tin của cơ quan, đơn vị, địa phương mình theo quy định tại Quy chế này.

2. Thường xuyên kiểm tra, rà soát việc quản trị, vận hành các hệ thống thông tin của cơ quan, đơn vị, địa phương mình.

3. Căn cứ Chỉ thị số 02/CT-TTg ngày 26/4/2022 của Thủ tướng Chính phủ về phát triển Chính phủ điện tử hướng tới Chính phủ số, thúc đẩy chuyển đổi số quốc gia, đơn vị xem xét ban hành Quy chế bảo đảm an toàn thông tin tại cơ quan, đơn vị, địa phương mình.

4. Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền.

5. Cử đầu mối phối hợp với Sở Thông tin và Truyền thông tham gia các hoạt động bảo đảm an toàn thông tin mạng trên địa bàn tỉnh.

6. Hàng năm, đề xuất nhu cầu đào tạo, tập huấn, bồi dưỡng kiến thức về đảm bảo an toàn thông tin.

7. Thực hiện báo cáo định kỳ theo quy định tại Điều 21 Quy chế này, báo cáo đột xuất các hoạt động bảo đảm an toàn thông tin mạng của cơ quan, đơn vị, địa phương gửi về Sở Thông tin và Truyền thông để tổng hợp, báo cáo Ủy ban nhân dân tỉnh theo quy định.

Điều 24. Khen thưởng, xử lý vi phạm

1. Các cơ quan, đơn vị khen thưởng đối với tổ chức, cá nhân triển khai tốt các hoạt động bảo đảm an toàn thông tin mạng theo quy định của pháp luật về thi đua, khen thưởng và quy chế khen thưởng tại cơ quan, đơn vị.

2. Cơ quan, cá nhân vi phạm Quy chế này, thì tùy theo tính chất và mức độ vi phạm sẽ bị xem xét xử lý kỷ luật theo quy định của pháp luật.

Điều 25. Điều khoản thi hành

1. Sở Thông tin và Truyền thông chịu trách nhiệm chủ trì, phối hợp với các cơ quan, đơn vị có liên quan hướng dẫn, triển khai và kiểm tra, đôn đốc việc thực hiện Quy chế này.

2. Thủ trưởng các cơ quan, đơn vị trên địa bàn tỉnh và tổ chức có liên quan trong phạm vi chức năng nhiệm vụ của mình, có trách nhiệm tổ chức triển khai thực hiện nghiêm Quy chế.

3. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc cần sửa đổi, bổ sung, các cơ quan, đơn vị, địa phương phản ánh về Sở Thông tin và Truyền thông để tổng hợp, báo cáo Ủy ban nhân dân tỉnh xem xét, quyết định.

Điều 26. Xây dựng và công bố Quy chế

1. Quy chế được lấy ý kiến cấp có thẩm quyền, đơn vị liên quan trước khi công bố áp dụng.

2. Quy chế được công bố trước khi áp dụng.

3. Tổ chức tuyên truyền, phổ biến cho toàn bộ công chức, viên chức trong tổ chức.

Điều 27. Rà soát, cập nhật, bổ sung Quy chế

1. Định kỳ hàng năm hoặc khi có thay đổi chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung Quy chế bảo đảm an toàn thông tin.

2. Có hồ sơ lưu lại thông tin phản hồi của đối tượng áp dụng. Trong quá trình thực hiện, nếu có những vấn đề vướng mắc cần sửa đổi, bổ sung, Sở Thông tin và Truyền thông tổng hợp, đề xuất Ủy ban nhân dân tỉnh xem xét, quyết định./.