UBND TỈNH NINH BÌNH
TRUNG TÂM XÚC TIẾN ĐẦU TƯ VÀ THƯƠNG MẠI
Số: 221 /QĐ-TTXTĐTTM

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

Ninh Bình, ngày 18 tháng 5 năm 2026

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn Hệ thống thông tin của Trung tâm Xúc tiến đầu tư và Thương mại tỉnh Ninh Bình

GIÁM ĐỐC TRUNG TÂM XÚC TIẾN ĐẦU TƯ VÀ THƯƠNG MẠI TỈNH NINH BÌNH

Căn cứ Luật tổ chức Chính quyền địa phương ngày 16/6/2025;

Căn cứ Luật Công nghệ thông tin ngày 29/06/2006;

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2025;

Căn cứ Luật An ninh mạng số 24/2018/QH14 ngày 12/6/2018;

Căn cứ Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ về hoạt động ngăn chặn xung đột thông tin trên mạng;

Căn cứ Nghị định số 53/2016/NĐ-CP ngày 15/08/2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

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 Thông tư số 31/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông về việc 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 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 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 1518/QĐ-UBND ngày 14/4/2025 của UBND tỉnh Ninh Bình ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Trung tâm Xúc tiến đầu tư và Thương mại tỉnh Ninh Bình;

Theo đề nghị của Trưởng phòng Hành chính.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn Hệ thống thông tin của Trung tâm Xúc tiến đầu tư và Thương mại tỉnh Ninh Bình.

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

Điều 3. Các đồng chí Lãnh đạo Trung tâm; Trưởng phòng Hành chính; Trưởng các phòng chuyên môn thuộc Trung tâm và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như điều 3;
- Lãnh đạo Trung tâm;
- Trang TTĐT Trung tâm;
- Lưu VT. HL.

GIÁM ĐỐC

ỦY BAN NHÂN DÂN TỈNH NINH BÌNH
TRUNG TÂM XÚC TIẾN ĐẦU TƯ VÀ THƯƠNG MẠI TỈNH NINH BÌNH

Trương Quốc Bảo

UBND TỈNH NINH BÌNH
TRUNG TÂM XÚC TIẾN ĐẦU TƯ VÀ THƯƠNG MẠI

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

QUY CHẾ
Bảo đảm an toàn Hệ thống thông tin của Trung tâm Xúc tiến đầu tư và thương mại tỉnh Ninh Bình

(Ban hành kèm theo Quyết định số 221/QĐ-TTXTĐTTM ngày 18 tháng 5 năm 2026 của Trung tâm Xúc tiến đầu tư và thương mại tỉnh Ninh Bình)

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 về bảo đảm an toàn Hệ thống thông tin của Trung tâm Xúc tiến đầu tư và thương mại tỉnh Ninh Bình.

2. Đối tượng áp dụng

a) Các phòng thuộc Trung tâm Xúc tiến đầu tư và thương mại tỉnh Ninh Bình; viên chức, người lao động và các tổ chức, cá nhân tham gia vận hành, khai thác các Hệ thống thông tin của Trung tâm.

b) Cơ quan, tổ chức, cá nhân có kết nối, sử dụng các Hệ thống thông tin của Trung tâm Xúc tiến đầu tư và thương mại tỉnh Ninh Bình.

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 thuộc Trung tâm.

Điều 2. Giải thích từ ngữ

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

1. *An toàn thông tin mạng* là sự bảo vệ thông tin, Hệ thống thông tin trên mạng tránh bị truy cập, 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.

2. *Mạng* là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

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

4. *Hệ thống thông tin quan trọng quốc gia* là Hệ thống thông tin mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới quốc phòng, an ninh quốc gia.

5. *Chủ quản Hệ thống thông tin* là cơ quan, tổ chức, cá nhân có thẩm quyền quản lý trực tiếp đối với Hệ thống thông tin.

6. *Xâm phạm an toàn thông tin mạng* là hành vi truy nhập, sử dụng, tiết lộ, làm gián đoạn, sửa đổi, phá hoại trái phép thông tin, Hệ thống thông tin.

7. *Sự cố an toàn thông tin mạng* là việc thông tin, Hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

8. *Rủi ro an toàn thông tin mạng* là những nhân tố chủ quan hoặc khách quan có khả năng ảnh hưởng tới trạng thái an toàn thông tin mạng.

9. *Đánh giá rủi ro an toàn thông tin mạng* là việc phát hiện, phân tích, ước lượng mức độ tổn hại, mối đe dọa đối với thông tin, Hệ thống thông tin.

10. *Quản lý rủi ro an toàn thông tin mạng* là việc đưa ra các biện pháp nhằm giảm thiểu rủi ro an toàn thông tin mạng.

11. *Phần mềm độc hại* là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ Hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong Hệ thống thông tin.

12. *Hệ thống lọc phần mềm độc hại* là tập hợp phần cứng, phần mềm được kết nối vào mạng để phát hiện, ngăn chặn, lọc và thống kê phần mềm độc hại.

13. *Địa chỉ điện tử* là địa chỉ được sử dụng để gửi, nhận thông tin trên mạng bao gồm địa chỉ thư điện tử, số điện thoại, địa chỉ Internet và hình thức tương tự khác.

14. *Xung đột thông tin* là việc hai hoặc nhiều tổ chức trong nước và nước ngoài sử dụng biện pháp công nghệ, kỹ thuật thông tin gây tổn hại đến thông tin, Hệ thống thông tin trên mạng.

15. *Thông tin cá nhân* là thông tin gắn với việc xác định danh tính của một người cụ thể.

16. *Chủ thể thông tin cá nhân* là người được xác định từ thông tin cá nhân đó.

17. *Xử lý thông tin cá nhân* là việc thực hiện một hoặc một số thao tác thu thập, biên tập, sử dụng, lưu trữ, cung cấp, chia sẻ, phát tán thông tin cá nhân trên mạng nhằm mục đích thương mại.

18. *Mật mã dân sự* là kỹ thuật mật mã và sản phẩm mật mã được sử dụng để bảo mật hoặc xác thực đối với thông tin không thuộc phạm vi bí mật nhà nước.

19. *Sản phẩm an toàn thông tin mạng* là phần cứng, phần mềm có chức năng bảo vệ thông tin, Hệ thống thông tin.

20. *Dịch vụ an toàn thông tin mạng* là dịch vụ bảo vệ thông tin, hệ thống thông tin.

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

1. Mục tiêu

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 Hệ thống thông tin.

2. Nguyên tắc

a) Cơ quan, tổ chức thuộc đối tượng áp dụng Quy chế này có trách nhiệm bảo đảm an toàn thông tin trong phạm vi xử lý công việc của mình theo quy định của pháp luật và Quy chế này.

b) Bảo đảm an toàn thông tin là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục trong quá trình thu thập, xử lý, lưu trữ và sử dụng thông tin.

c) Việc bảo đảm an toàn Hệ thống thông tin phải được thực hiện đồng bộ, tổng thể, tránh đầu tư chồng chéo, lãng phí.

Điều 4. Những hành vi nghiêm cấm

1. Thực hiện các hành vi bị nghiêm cấm quy định tại Điều 7, Luật An toàn thông tin mạng và Điều 8 Luật An ninh mạng.

2. Tự ý đấu nối thiết bị mạng, thiết bị phát sóng, thiết bị cấp phát địa chỉ mạng của cá nhân vào mạng nội bộ của cơ quan.

3. Tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin đã được cài đặt trên thiết bị công nghệ thông tin phục vụ công việc.

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

1. Trung tâm giao Phòng Hành chính là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền trong công tác bảo đảm an toàn thông tin.

2. Phòng Hành chính chủ trì tiếp nhận, xử lý sự cố an toàn thông tin; phối hợp với các đơn vị liên quan trong công tác ứng cứu sự cố.

3. Các phòng chuyên môn, viên chức và người lao động có trách nhiệm phối hợp khi có yêu cầu.

Điều 6. Bảo đảm nguồn nhân lực

1. Viên chức làm công tác công nghệ thông tin, an toàn thông tin phải có chuyên môn phù hợp với vị trí việc làm.

2. Định kỳ hằng năm tham gia đào tạo, tập huấn về an toàn thông tin do cơ quan có thẩm quyền tổ chức.

3. Viên chức quản trị hệ thống phải thực hiện đầy đủ trách nhiệm về quản lý tài khoản, truy cập, bảo mật và giám sát hệ thống.

4. Người sử dụng phải chấp hành đầy đủ các quy định về bảo đảm an toàn thông tin và chịu trách nhiệm đối với tài khoản được cấp.

5. Khi viên chức, người lao động nghỉ việc hoặc thay đổi vị trí công tác phải thực hiện thu hồi tài khoản, quyền truy cập và bàn giao đầy đủ tài sản, dữ liệu liên quan.

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. Xây dựng các tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành Hệ thống thông tin. Trong đó, phân công rõ trách nhiệm, nhiệm vụ của các đối tượng tham gia sử dụng, khai thác và vận hành Hệ thống thông tin.

2. Xây dựng các tài liệu mô tả thiết kế và các thành phần của Hệ thống thông tin. Thường xuyên cập nhật, bổ sung các thành phần Hệ thống thông tin khi thực hiện nâng cấp, mở rộng.

3. Khi lựa chọn các giải pháp công nghệ phải xây dựng các tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin. Tổ chức xin ý kiến các đơn vị quản lý về an toàn thông tin hoặc các chuyên gia có uy tín trong lĩnh vực an toàn thông tin.

4. 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.

5. Khi thiết kế xây dựng, nâng cấp, mở rộng Hệ thống thông tin, chủ quản Hệ thống thông tin phải đánh giá lại phương án bảo đảm an toàn thông tin trong hồ sơ thiết kế và gửi đơn vị chuyên trách về an toàn thông tin của chủ quản Hệ thống thông tin thẩm định và phê duyệt cấp độ cho Hệ thống thông tin trước khi trình cấp có thẩm quyền phê duyệt dự án.

6. Đánh giá, phân loại cấp độ an toàn thông tin của Hệ thống thông tin

a) Chủ quản Hệ thống thông tin có trách nhiệm tổ chức đánh giá, phân loại cấp độ an toàn thông tin của Hệ thống thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống theo cấp độ (gọi tắt là Nghị định số 85/2016/NĐ-CP) và Thông tư số 24/2020/TT-

BTTTT ngày 09/9/2020 của Bộ Thông tin và Truyền thông để áp dụng phương án bảo đảm an toàn thông tin phù hợp.

b) Hồ sơ đề xuất cấp độ bao gồm các tài liệu được quy định tại Điều 15, Nghị định số 85/2016/NĐ-CP, gửi đơn vị chuyên trách về an toàn thông tin của chủ quản Hệ thống thông tin hoặc đơn vị chuyên trách về an toàn thông tin của Ủy ban nhân dân tỉnh thẩm định, trình cấp có thẩm quyền phê duyệt.

7. Trước khi đưa vào vận hành, khai thác Hệ thống thông tin, Chủ quản Hệ thống thông tin phải thực hiện kiểm thử hoặc vận hành thử trước khi đưa vào sử dụng. Kết quả kiểm thử, vận hành thử phải được lập thành văn bản và tuân thủ theo quy định tại Điều 10, Thông tư số 24/2020/TT-BTTTT ngày 09/9/2020 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về công tác triển khai, giám sát công tác triển khai và nghiệm thu dự án đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước.

Điều 8. Phát triển phần mềm thuê khoán

1. Có biên bản, điều khoản hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán.

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. Khi thay đổi mã nguồn, kiến trúc phần mềm thực hiện kiểm tra, đánh giá an toàn thông tin cho phần mềm.

6. Có cam kết của bên phát triển về bảo đảm tính bí mật và bản quyền của phần mềm phát triển.

Điều 9. Thử nghiệm và nghiệm thu hệ thống

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

2. Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống.

3. Có bộ phận có trách nhiệm thực hiện thử nghiệm 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 thử nghiệm 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.

Điều 10. Bảo vệ bí mật nhà nước trong hoạt động ứng dụng công nghệ thông tin

1. Quy định về soạn thảo, in ấn, phát hành và sao chụp tài liệu mật

a) Không được sử dụng máy tính nối mạng Internet để soạn thảo văn bản; chuyển giao, lưu trữ thông tin có nội dung thuộc bí mật nhà nước; cung cấp tin, tài liệu và đưa thông tin bí mật nhà nước trên Trang thông tin điện tử;

b) Không được in, sao chụp tài liệu bí mật nhà nước trên các thiết bị kết nối mạng internet;

c) Phải bố trí 01 máy tính riêng, không kết nối mạng nội bộ và mạng Internet dùng để quản lý, soạn thảo các tài liệu mật của nhà nước theo quy định.

2. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các phòng thuộc Trung tâm phải báo cáo cho người có thẩm quyền. Không được cho phép các tổ chức, cá nhân không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

3. Trước khi thanh lý các máy tính trong các cơ quan nhà nước, cán bộ chuyên trách công nghệ thông tin phải dùng các biện pháp kỹ thuật xóa bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

Chương III

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

Điều 11. Quản lý an toàn mạng

1. Quản lý, vận hành hoạt động bình thường của hệ thống thông tin 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. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố

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.

Định kỳ cập nhật; sao lưu dự phòng các tập tin cấu hình hệ thống và khôi phục hệ thống sau khi xảy ra sự cố:

Sao lưu định kỳ thực hiện sao lưu hàng ngày (đối với cơ sở dữ liệu) và hàng tháng đối với tập tin cấu hình hệ thống.

Cập nhật: thực hiện khi có bản cập nhật mới của đơn vị cung cấp hệ thống.

3. Truy cập và quản lý cấu hình hệ thống

a) Viên chức và người lao động vận hành truy cập, khai thác thông tin tại Hệ thống thông tin 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) Tổ Công nghệ thông tin có quyền truy cập và quản lý cấu hình hệ thống thực hiện một số nhiệm vụ sau:

- Cấu hình tối ưu, tăng cường bảo mật cho thiết bị Hệ thống thông tin.
- 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.
- Tham mưu xây dựng quy trình quản lý an toàn người sử dụng đầu cuối.

Điều 12. Quản lý an toàn dữ liệu

1. Yêu cầu an toàn đối với phương pháp mã hóa

a) Đơn vị 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.

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

2. Phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa.

3. Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu.

4. Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ

a) Ban hành quy định về trao đổi thông tin tối thiểu gồm: Phân loại thông tin theo mức độ nhạy cảm; quyền và trách nhiệm của cá nhân khi tiếp cận thông

tin; biện pháp Bảo đảm tính toàn vẹn, bảo mật khi truyền nhận, xử lý, lưu trữ thông tin; chế độ bảo quản thông tin.

b) Các thông tin, tài liệu, dữ liệu nhạy cảm phải được mã hóa trước khi trao đổi, truyền nhận qua mạng máy tính.

c) Thực hiện các biện pháp quản lý, giám sát và kiểm soát chặt chẽ các trang/cổng thông tin điện tử cung cấp thông tin, dịch vụ, giao dịch trực tuyến cho các tổ chức, cá nhân bên ngoài.

d) Thực hiện biện pháp bảo vệ trang thiết bị, phần mềm phục vụ trao đổi thông tin nội bộ nhằm hạn chế việc xâm nhập, khai thác bất hợp pháp các thông tin nhạy cảm.

5. 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 của hệ thống: Đơn vị quản trị hệ thống thực hiện xây dựng Tài liệu hướng dẫn sao lưu cụ thể đối với từng hệ thống.

6. Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ:

a) 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 (nếu có).

b) Thực hiện sao lưu dữ liệu định kỳ: Cán bộ phụ trách sao lưu thực hiện sao lưu định kỳ theo phương án sao lưu đã được phê duyệt.

c) Kiểm tra định kỳ: Dữ liệu sao lưu phải được lưu trữ an toàn và được kiểm tra thường xuyên Bảo đảm sẵn sàng cho việc sử dụng khi cần. Kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu.

Điều 13. Quản lý an toàn thiết bị đầu cuối

Quy định về quản lý an toàn thiết bị đầu cuối bao gồm các nội dung:

1. Thông tin về thiết bị đầu cuối (tên, chủng loại, địa chỉ MAC, địa chỉ IP) phải được quản lý và cập nhật.

2. Các thiết bị đầu cuối phải được quản lý khi kết nối vào hệ thống mạng theo địa chỉ MAC, IP.

3. Khi truy cập và sử dụng thiết bị đầu cuối từ xa phải có cơ chế xác thực và sử dụng giao thức mạng an toàn.

4. Việc cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt.

Điều 14. Quản lý phòng, chống phần mềm độc hại

1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; Chế độ tự động quét mã độc khi sao chép, mở các tập tin.

2. Khi gửi văn bản điện tử gửi qua hệ thống thư điện tử phải có định dạng theo Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước như: (.txt), (.doc), (.odt), (.pdf) và các định dạng khác theo quy định, không được gửi các file thực thi (.com), (.bat), (.exe) ….

3. Viên chức và người lao động trong cơ quan phải được hướng dẫn về phòng chống mã độc, các rủi ro do mã độc gây ra; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của cơ quan.

4. Tất cả các máy tính của đơn vị phải được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động.

5. Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: Máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu…), người sử dụng phải báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.

6. Phần mềm ứng dụng trước khi được cài đặt, sử dụng phải được kiểm tra xem có phần mềm độc hại tồn tại hay không. Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.

7. Định kỳ hằng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; Thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.

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

1. Triển khai hệ thống giám sát Trung tâm phải đáp ứng yêu cầu tại khoản 1, Điều 5 Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông về Quy định hoạt động giám sát an toàn Hệ thống thông tin.

2. Thông tin giám sát và danh mục các đối tượng giám sát phải đáp ứng yêu cầu tại khoản 2, Điều 5, Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông. Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát.

3. Thực thi nhiệm vụ giám sát theo quy định tại khoản 3, Điều 5, Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông.

4. Định kỳ hằng năm tổ chức nâng cao năng lực hoạt động giám sát theo quy định tại Điều 9, Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông.

5. Chủ quản Hệ thống thông tin có trách nhiệm giám sát an toàn thông tin theo quy định tại Điều 14, Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông.

Điều 16. Quản lý điểm yếu an toàn thông tin

1. Đơn vị hoặc Bộ phận chuyên trách về an toàn thông tin có trách nhiệm

a) Quản lý thông tin điểm yếu an toàn thông tin đối với từng thành phần có trong hệ thống (hệ điều hành, máy chủ, ứng dụng, dịch vụ…); Phân loại mức độ nguy hiểm của điểm yếu; Xây dựng phương án và quy trình xử lý đối với từng mức độ nguy hiểm của điểm yếu.

b) Báo cáo Lãnh đạo, cán bộ quản lý ngay khi phát hiện điểm yếu an toàn thông tin ở mức độ nghiêm trọng. Thực hiện cảnh báo và xử lý điểm yếu an toàn thông tin theo chỉ đạo. Việc xử lý điểm yếu an toàn thông tin phải bảo đảm không giảm ảnh hưởng/gián đoạn hoạt động của hệ thống.

c) Xây dựng phương án xử lý tạm thời đối với trường hợp điểm yếu an toàn thông tin chưa được khắc phục và phương án khôi phục hệ thống trong trường hợp xử lý điểm yếu thất bại.

d) Có trách nhiệm phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin đối với các điểm yếu khi cần thiết.

2. Định kỳ hằng năm kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ Hệ thống thông tin; Thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong hệ thống.

3. Hoạt động đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thực hiện theo quy định tại điểm c, khoản 2, Điều 20, 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 và Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông về việc quy định chi tiết và hướng dẫn một số điều của nghị định số 85/2016/NĐ-CP.

Điều 17. Quản lý sự cố an toàn thông tin

1. Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ 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. Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13, 14, Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ về việc Ban hành Quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng Quốc gia.

3. Xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16, Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ về việc Ban hành Quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng Quốc gia.

4. Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về an toàn thông tin; Hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất an toàn thông tin; Yêu cầu ngừng hoạt động một phần hoặc toàn bộ các Hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về an toàn thông tin; Phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo.

5. 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.

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

1. Kết nối máy 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 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) Máy tính, thiết bị đầu cuối phải được xử lý điểm yếu an toàn thông tin, cấu hình bảo mật trước khi kết nối vào hệ thống.

2. Trong quá trình sử dụng

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao.

b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng.

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

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

3. Quy định, quy trình về Kết thúc vận hành, khai thác, thanh lý, hủy bỏ bao gồm các nội dung sau:

a) Thiết bị CNTT có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng phải được cán bộ vận hành kiểm tra. 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.

c) Các phương tiện và thiết bị CNTT: 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 phải xóa sạch dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng.

Chương IV

KIỂM TRA, ĐÁNH GIÁ VÀ QUẢN LÝ RỦI RO

Điều 19. Nội dung, hình thức kiểm tra, đánh giá

1. Mục đích và phạm vi áp dụng:

Nhằm nhận diện, đánh giá, xử lý và giám sát các rủi ro có thể ảnh hưởng đến an toàn thông tin của hệ thống mạng nội bộ (LAN) và các Hệ thống thông tin có liên quan của cơ quan.

2. Nội dung kiểm tra, đánh giá

a) Kiểm tra việc thực hiện các nội dung tại quy chế này; kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn Hệ thống thông tin theo cấp độ.

b) Đánh giá hiệu quả của biện pháp bảo đảm an toàn Hệ thống thông tin.

c) Đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống.

d) Kiểm tra, đánh giá khác do chủ quản Hệ thống thông tin quy định và theo quy định của hệ thống an toàn thông tin.

3. Hình thức kiểm tra, đánh giá

a) Kiểm tra, đánh giá định kỳ theo kế hoạch của chủ quản Hệ thống thông tin, theo kế hoạch của Trung tâm Xúc tiến đầu tư và thương mại tỉnh Ninh Bình và đơn vị chuyên trách về an toàn thông tin của tỉnh.

b) Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền.

4. Cấp có thẩm quyền yêu cầu kiểm tra, đánh giá.

a) Đơn vị chuyên trách an toàn thông tin.

b) Ủy ban nhân dân tỉnh.

c) Trung tâm Xúc tiến đầu tư và thương mại tỉnh Ninh Bình giao nhiệm vụ kiểm tra về an toàn thông tin cho Phòng Hành chính thực hiện.

5. 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 nhiệm vụ kiểm tra, đánh giá.

6. 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.

Điều 20. Kế hoạch kiểm tra hằng năm

1. Phòng Hành chính được giao chủ trì, phối hợp với các đơn vị liên quan tiến hành kiểm tra công tác bảo đảm an toàn thông tin của Trung tâm theo Kế hoạch công tác hằng năm.

2. Tiến hành kiểm tra đột xuất các phòng, đơn vị trực thuộc khi có dấu hiệu vi phạm an toàn đối với các Hệ thống thông tin của Trung tâm.

Chương V
BÁO CÁO, CHIA SẺ THÔNG TIN

Điều 21. Chế độ báo cáo

1. Báo cáo định kỳ

a) Báo cáo an toàn thông tin định kỳ hằng năm gồm các nội dung quy định tại Điều 14, Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông.

b) Báo cáo hoạt động giám sát của chủ quản Hệ thống thông tin định kỳ 6 tháng theo mẫu tại Phụ lục 2, Thông tư số 31/2017/TT-BTTTT.

2. Báo cáo đột xuất: Báo cáo về công tác khắc phục mã độc, lỗ hổng, điểm yếu, triển khai cảnh báo an toàn thông tin và các báo cáo đột xuất khác theo yêu cầu của các cơ quan quản lý nhà nước về an toàn thông tin.

Điều 22. Chia sẻ thông tin

Việc chia sẻ dữ liệu số của các Hệ thống thông tin với các cơ quan nhà nước được thực hiện theo quy định tại Nghị định số 47/2020/NĐ-CP ngày 09/4/2020 của Chính phủ về việc quản lý, kết nối và chia sẻ dữ liệu của cơ quan nhà nước.

Chương VI
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 23. Đơn vị vận hành

1. Thực hiện trách nhiệm của đơn vị vận hành Hệ thống thông tin theo quy định tại Điều 22, Nghị định số 85/2016/NĐ-CP, tại Quy chế này và các nhiệm vụ do chủ quản Hệ thống thông tin phân công.

2. Chỉ đạo các phòng thuộc Trung tâm thực hiện quản lý ứng dụng; quản lý dữ liệu; triển khai và hỗ trợ kỹ thuật, triển khai công tác bảo đảm an toàn thông tin trong tất cả các công đoạn liên quan đến Hệ thống thông tin.

3. Lập hồ sơ đề xuất cấp độ, gửi về Đơn vị hoặc Bộ phận chuyên trách về an toàn thông tin của chủ quản Hệ thống thông tin thẩm định *(theo quy định tại Nghị định 85/2016/NĐ-CP).*

Điều 24. Trách nhiệm của đơn vị, bộ phận chuyên trách, bán chuyên trách về an toàn thông tin

1. Phòng Hành chính được giao; các phòng thuộc Trung tâm thực thi nhiệm vụ bảo đảm an toàn thông tin và ứng cứu sự cố an toàn thông tin mạng theo các quy định tại Quy chế này và hướng dẫn các viên chức và người lao động của Trung tâm Xúc tiến đầu tư và thương mại tỉnh Ninh Bình triển khai Bảo đảm an toàn, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin tại đơn vị mình.

2. Đơn vị chuyên trách về an toàn thông tin thẩm định hồ sơ cấp độ 1, 2 *(quy định tại khoản 1, Điều 12 của Nghị định số 85/2016/NĐ-CP)* và gửi hồ sơ cấp độ về Công an tỉnh Ninh Bình để phê duyệt hồ sơ cấp độ.

Điều 25. Trách nhiệm của đơn vị cung cấp dịch vụ

1. Đơn vị cung cấp dịch vụ có trách nhiệm bảo đảm cung cấp đầy đủ các thành phần, chức năng; Thiết kế, thiết lập hệ thống đáp ứng các yêu cầu kỹ thuật các cấp độ theo tiêu chuẩn quy định.

2. Quản lý, vận hành, bảo đảm an toàn thông tin cho các thành phần hệ thống thuộc phạm vi quản lý của mình tuân thủ các quy định tại Quy chế này.

3. Phối hợp đơn vị vận hành lập hồ sơ cấp độ của Hệ thống thông tin, để chuyển đến đơn vị, các cấp có thẩm quyền thẩm định, phê duyệt hệ thống.

Điều 26. Trách nhiệm của đơn vị, tổ chức, cá nhân sử dụng hệ thống

Tổ chức, cá nhân sử dụng hệ thống thông tin có trách nhiệm tuân thủ các quy định về bảo đảm an toàn thông tin theo Quy chế này.

Điều 27. Bảo đảm an ninh mạng

Thực hiện theo Điều 12, Điều 13, Điều 14 của Quyết định số 1512/QĐ-BTTTT ngày 05/10/2021 của Bộ trưởng Bộ Thông tin và Truyền thông về việc ban hành Quy chế bảo đảm an toàn thông tin mạng và an ninh mạng; các quy định khác có liên quan.

Điều 28. Trách nhiệm của bộ phận phụ trách công tác Bảo đảm an toàn thông tin

1. Chỉ định nhân sự phụ trách công tác Bảo đảm an toàn thông tin của Trung tâm Xúc tiến đầu tư và thương mại tỉnh Ninh Bình.

2. Phân định vai trò, trách nhiệm, cơ chế phối hợp của bộ phận với các tổ chức, cá nhân trong và ngoài cơ quan, đơn vị.

Chương VII

TỔ CHỨC THỰC HIỆN

Điều 29. Tổ chức triển khai Quy chế

1. Quy chế này có hiệu lực thi hành kể từ ngày ký ban hành.

2. Trong quá trình thực hiện nếu phát sinh khó khăn, vướng mắc, các đơn vị phản ánh về Phòng Hành chính để tổng hợp, tham mưu lãnh đạo Trung tâm xem xét, sửa đổi, bổ sung.

Điều 30. Rà soát, cập nhật, bổ sung Quy chế

1. Định kỳ 03 năm hoặc khi có thay đổi chính sách về an toàn thông tin phải tổ chức rà soát, cập nhật, bổ sung Quy chế.

2. Có hồ sơ lưu lại thông tin phản hồi của đối tượng áp dụng trong quá trình thực hiện.

3. Quy chế này được phổ biến đến toàn thể viên chức, người lao động và các tổ chức, cá nhân có liên quan.

Điều 31. Bộ phận chuyên trách về an toàn thông tin

1. Giao Phòng Hành chính thực hiện nhiệm vụ tham mưu, tổ chức triển khai các nội dung về bảo đảm an toàn thông tin.

2. Chủ trì phối hợp kiểm tra công tác bảo đảm an toàn thông tin định kỳ hoặc đột xuất theo chỉ đạo.

Điều 32. Trách nhiệm của các phòng chuyên môn

1. Căn cứ Quy chế này, lãnh đạo các phòng chuyên môn có trách nhiệm tổ chức triển khai thực hiện trong phạm vi quản lý.

2. Phòng Hành chính có trách nhiệm theo dõi, đôn đốc, kiểm tra, đánh giá việc thực hiện Quy chế.

3. Trong quá trình thực hiện nếu có khó khăn, vướng mắc, các phòng chuyên môn phản ánh về Trung tâm (qua Phòng Hành chính) để tổng hợp, báo cáo cấp có thẩm quyền xem xét, giải quyết./.