SỞ KH&CN BÌNH ĐỊNH
TRUNG TÂM THÔNG TIN - ỨNG DỤNG KHOA HỌC VÀ CÔNG NGHỆ

Số:276 /QĐ-TTƯD

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

Bình Định, ngày28 tháng 10 năm 2024

QUYẾT ĐỊNH
Về việc ban hành Quy chế bảo đảm an toàn thông tin của Trung tâm Thông tin - Ứng dụng KH&CN Bình Định

GIÁM ĐỐC TRUNG TÂM THÔNG TIN - ỨNG DỤNG KHOA HỌC VÀ CÔNG NGHỆ

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

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

Căn cứ Quyết định số 22/2021/QĐ-UBND ngày 11/6/2021 của Ủy ban nhân dân tỉnh Bình Định về việc ban hành quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Bình Định;

Căn cứ Quyết định số 3166/QĐ-UBND ngày 04/09/2019 của UBND tỉnh về việc Ban hành Quy chế Tổ chức và hoạt động của Trung tâm Thông tin - Ứng dụng khoa học và công nghệ Bình Định trực thuộc Sở Khoa học và Công nghệ;

Xét đề nghị của Phụ trách phòng Thông tin – Thống kê.

QUYẾT ĐỊNH:

Điều 1. Ban hành "Quy chế bảo đảm an toàn thông tin của Trung tâm Thông tin - Ứng dụng khoa học và công nghệ Bình Định".

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

Điều 3. Phụ trách các Phòng, Trạm, viên chức và lao động hợp đồng của Trung tâm chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như điều 3;
- Lãnh đạo Trung tâm;
- Lưu P.TTTK, VT.

GIÁM ĐỐC

SỞ KHOA HỌC VÀ CÔNG NGHỆ TỈNH BÌNH ĐỊNH
TRUNG TÂM THÔNG TIN-ỨNG DỤNG KHOA HỌC VÀ CÔNG NGHỆ BÌNH ĐỊNH

Trương Ngọc Phong

SỞ KH&CN BÌNH ĐỊNH
TRUNG TÂM THÔNG TIN - ỨNG DỤNG KHOA HỌC VÀ CÔNG NGHỆ

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

QUY CHẾ
Bảo đảm an toàn thông tin của Trung tâm Thông tin - Ứng dụng KH&CN

(Kèm theo Quyết định số /QĐ-TTƯD ngày tháng 10 năm 2024 của Trung tâm Thông tin - Ứng dụng KH&CN)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Mục đích bảo đảm an toàn, an ninh thông tin

1. Giảm thiểu được các nguy cơ gây sự cố mất an toàn thông tin và đảm bảo an ninh thông tin trong quá trình tác nghiệp của viên chức và lao động hợp đồng.

2. Công tác đảm bảo an toàn, an ninh thông tin, bảo mật trên môi trường mạng là một trong những nhiệm vụ trọng tâm để đảm bảo thành công trong việc ứng dụng công nghệ thông tin trong hoạt động của Trung tâm Thông tin - Ứng dụng KH&CN.

Điều 2. Phân nhóm sự cố an toàn thông tin mạng

1. Tấn công mạng: Tấn công làm quá tải hệ thống, gây gián đoạn dịch vụ, thường do lỗ hổng bảo mật chưa được vá.

2. Mã độc/phần mềm độc hại: Phần mềm độc hại tự sao chép, phá hủy hoặc mã hóa dữ liệu, đôi khi đòi tiền chuộc để giải mã.

3. Mất mát/rò rỉ dữ liệu: Mất dữ liệu quan trọng hoặc rò rỉ thông tin do lỗi hệ thống hoặc hành vi sai.

4. Chính sách/quy trình: Vi phạm quy định an ninh như sử dụng phần mềm không hợp pháp hoặc quản lý dữ liệu không đúng.

5. Tấn công xã hội: Lừa người dùng cung cấp thông tin cá nhân hoặc quyền truy cập.

Điều 3. Phạm vi, đối tượng áp dụng

Quy chế này áp dụng đối với tất cả các viên chức, lao động hợp đồng khi tham gia khai thác, sử dụng hệ thống công nghệ thông tin của Trung tâm.

Chương II

QUY ĐỊNH ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 4. Các biện pháp quản lý vận hành trong công tác đảm bảo an toàn, an ninh thông tin

1. Đối với Lãnh đạo Trung tâm và Lãnh đạo phòng:

a. Trang bị đầy đủ các kiến thức bảo mật cơ bản cho viên chức, lao động hợp đồng trước khi cho phép truy nhập và sử dụng hệ thống thông tin.

b. Bố trí cán bộ chuyên trách về an toàn hệ thống thông tin.

c. Xác định và phân bổ kinh phí chi thường xuyên cần thiết cho các hoạt động liên quan đến việc bảo vệ hệ thống thông tin, thông qua việc đầu tư các thiết bị tường lửa, các chương trình chống thư rác, phần mềm diệt vi rút máy tính trên các máy trạm, máy chủ và các công việc khác có liên quan đến việc bảo đảm an toàn, an ninh thông tin.

d. Bố trí ít nhất 01 máy vi tính riêng, không kết nối mạng nội bộ và mạng Internet dùng để quản lý, soạn thảo các tài liệu mật theo quy định.

2. Đối với cán bộ chuyên trách công nghệ thông tin tại Trung tâm:

a. Tham mưu chuyên môn và vận hành an toàn hệ thống thông tin của Trung tâm, triển khai các biện pháp bảo đảm an toàn, an ninh thông tin cho tất cả viên chức, người lao động trong Trung tâm. Thường xuyên tự nghiên cứu, cập nhật các kiến thức về an toàn, an ninh thông tin, nguy cơ tiềm ẩn có thể gây mất mát thông tin và các biện pháp phòng tránh khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

b. Thường xuyên cập nhật cấu hình chuẩn cho các thành phần của hệ thống thông tin, thiết lập cấu hình chặt chẽ nhất cho các sản phẩm an toàn thông tin nhưng vẫn duy trì yêu cầu hoạt động của hệ thống thông tin.

c. Khi tổ chức cấu hình hệ thống thông tin chỉ cung cấp những chức năng thiết yếu nhất, xác định rõ các chức năng, cổng giao tiếp mạng, giao thức và dịch vụ không cần thiết để cấm hoặc hạn chế không sử dụng.

d. Thường xuyên thực hiện việc theo dõi bản ghi nhật ký hệ thống và các sự việc khác có liên quan để đánh giá, báo cáo các rủi ro và mức độ nghiêm trọng các rủi ro đó. Các rủi ro đó có thể xảy ra do sự truy cập trái phép, sử dụng trái phép, mất, thay đổi hoặc phá hủy thông tin và hệ thống thông tin.

e. Kiểm soát chặt chẽ cài đặt phần mềm vào máy trạm và máy chủ.

3. Đối với viên chức, lao động hợp đồng:

a. Thường xuyên cập nhật những chính sách, thủ tục an toàn thông tin của Trung tâm cũng như thực hiện những hướng dẫn về an toàn, an ninh thông tin của cán bộ chuyên trách công nghệ thông tin.

b. Hạn chế việc sử dụng chức năng chia sẻ tài nguyên, khi sử dụng chức năng này cần bật thuộc tính bảo mật bằng mật khẩu và thực hiện việc thu hồi chức năng này khi đã sử dụng xong.

c. Các máy tính khi không sử dụng trong thời gian dài (quá 4 giờ làm việc) cần tắt máy hoặc ngưng kết nối mạng, để tránh bị các hacker lợi dụng, sử dụng chức năng điều khiển từ xa dùng máy tính của mình tấn công vào các hệ thống thông tin khác.

d. Khi mở các tập tin đính kèm theo thư điện tử, nếu biết rõ người gửi thư thì phải lưu tập tin vào máy tính rồi quét vi rút máy tính trước khi mở, không được mở các thư điện tử có tập tin đính kèm có nguồn gốc không rõ ràng vì rất có thể có vi rút máy tính, phần mềm gián điệp được đính kèm theo thư.

e. Phải đặt mật khẩu truy nhập vào máy tính của mình, đồng thời thiết lập chế độ bảo vệ tắt màn hình có sử dụng mật khẩu bảo vệ sau một khoảng thời gian nhất định không sử dụng máy tính. Sử dụng các thiết bị lưu trữ (usb, ổ cứng gắn ngoài...) an toàn, đúng cách để phòng ngừa virus, phần mềm gián điệp xâm nhập máy tính: khi gắn thiết bị lưu trữ vào máy tính, không được trực tiếp truy cập ngay mà phải quét vi rút trước.

Điều 5. Các biện pháp quản lý kỹ thuật cho công tác đảm bảo an toàn, an ninh thông tin

1. Tổ chức mô hình mạng: Cài đặt, cấu hình, tổ chức hệ thống mạng theo mô hình Clients/Server, hạn chế sử dụng mô hình mạng ngang hàng. Khi thiết lập các dịch vụ trên môi trường mạng Internet, chỉ cung cấp những chức năng thiết yếu nhất bảo đảm duy trì hoạt động của hệ thống thông tin.

2. Quản lý hệ thống mạng không dây: Khi thiết lập mạng không dây để kết nối với mạng cục bộ thông qua các điểm truy nhập (Access Point), cần thiết lập các tham số như: tên, SSID, mật khẩu, mã hóa dữ liệu và thông báo các thông tin liên quan đến Access Point để cơ quan sử dụng.

3. Tổ chức quản lý tài khoản của các hệ thống thông tin, bao gồm: Tạo mới, kích hoạt, sửa đổi, vô hiệu hóa và loại bỏ các tài khoản. Đồng thời tổ chức kiểm tra các tài khoản của hệ thống thông tin ít nhất 06 tháng/1 lần và triển khai các công cụ tự động để hỗ trợ việc quản lý các tài khoản của hệ thống thông tin. Hủy tài khoản, quyền truy nhập hệ thống thông tin, thu hồi lại tất cả các tài sản liên quan tới hệ thống thông tin (khóa, thẻ nhận dạng, thư mục lưu trữ) đối với viên chức, nhân viên đã chuyển công tác, chấm dứt hợp đồng lao động.

4. Quản lý đăng nhập hệ thống: Các hệ thống thông tin cần giới hạn số lần đăng nhập sai liên tiếp. Hệ thống tự động khóa tài khoản hoặc cô lập tài khoản trong một khoảng thời gian nhất định trước khi tiếp tục cho đăng nhập nếu liên tục đăng nhập sai vượt quá số lần quy định. Tổ chức theo dõi và kiểm soát tất cả các phương pháp truy nhập từ xa tới hệ thống thông tin bao gồm cả sự truy nhập có chức năng quản trị, tăng cường việc sử dụng mạng riêng ảo khi có nhu cầu

làm việc từ xa; yêu cầu người sử dụng đặt mật khẩu với độ an toàn cao, giám sát, nhắc nhở khuyến cáo nên thay đổi thường xuyên mật khẩu. Hệ thống thông tin cần có cơ chế kiểm tra, cho phép ứng với mỗi phương pháp truy nhập từ xa và cơ chế tự động giám sát, điều khiển các truy nhập từ xa.

5. Quản lý Logfile: Hệ thống thông tin cần ghi nhận các sự kiện cần thiết phục vụ quá trình kiểm soát: quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống, quá trình truy xuất hệ thống; ghi nhận đầy đủ các thông tin trong các bản ghi nhật ký để xác định những sự kiện nào đã xảy ra, nguồn gốc và các kết quả của sự kiện để có cơ chế bảo vệ và lưu giữ nhật ký trong một khoảng thời gian nhất định.

6. Chống mã độc, vi rút: Lựa chọn, triển khai các phần mềm chống vi rút, thư rác trên các máy chủ, các thiết bị di động trong mạng và những hệ thống thông tin xung yếu như: Cổng thông tin điện tử, thư điện tử, một cửa điện tử… để phát hiện, loại trừ những đoạn mã độc hại và hỗ trợ người sử dụng cài đặt các phần mềm này trên máy trạm. Thường xuyên cập nhật các phiên bản mới, các bản vá lỗi của các phần mềm chống virus để bảo đảm chương trình quét vi rút của cơ quan trên các máy chủ, máy trạm luôn được cập nhật mới nhất, phù hợp với quy trình và chính sách quản lý hệ thống thông tin của tổ chức, thiết lập chế độ quét thường xuyên ít nhất là hằng tuần.

7. Tổ chức quản lý tài nguyên: Kiểm tra, giám sát chức năng chia sẻ thông tin. Tổ chức cấp phát tài nguyên trên máy chủ theo danh mục thư mục cho từng phòng/trạm; khuyến cáo người sử dụng cân nhắc việc chia sẻ tài nguyên cục bộ trên máy đang sử dụng, tuyệt đối không được chia sẻ toàn bộ ổ cứng. Khi thực hiện việc chia sẻ tài nguyên trên máy chủ hoặc trên máy cục bộ nên sử dụng mật khẩu để bảo vệ thông tin.

8. Thiết lập cơ chế sao lưu và phục hồi máy chủ, máy trạm

a. Đối với máy trạm, máy chủ: Thực hiện việc sao lưu dữ liệu như hệ điều hành, các phần mềm ứng dụng, phần mềm chuyên ngành, cơ sở dữ liệu chuyên môn, quan trọng phục vụ công tác của Trung tâm bằng các phần mềm chuyên dụng.

b. Đối với máy chủ: Bảo đảm thiết lập cơ chế sao lưu và phục hồi hệ thống của máy chủ.

9. Xử lý khẩn cấp: Khi phát hiện hệ thống bị tấn công, thông qua các dấu hiệu như luồng tin tăng lên bất ngờ, nội dung trang chủ bị thay đổi, hệ thống hoạt động rất chậm khác thường, cần thực hiện các bước cơ bản sau:

a. Bước 1: Ngắt kết nối máy chủ ra khỏi mạng.

b. Bước 2: Sao chép logfile và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ (phục vụ cho công tác phân tích).

c. Bước 3: Khôi phục hệ thống bằng cách chuyển dữ liệu (backup) mới nhất để hệ thống hoạt động.

d. Bước 4: Báo cáo bằng văn bản cho cơ quan cấp trên quản lý trực tiếp.

10. Hệ thống thông tin cần có cơ chế ngăn chặn hoặc hạn chế các sự cố gây ra do tấn công từ chối dịch vụ (DoS, DDoS).

Điều 6. Quy trình ứng cứu sự cố an toàn thông tin mạng

1. Các đơn vị, cá nhân khi phát hiện dấu hiệu tấn công hoặc sự cố an toàn thông tin mạng cần nhanh chóng báo cho đơn vị vận hành hệ thống thông tin (thông qua chuyên trách công nghệ thông tin). Chuyên trách công nghệ thông tin có trách nhiệm cập nhật, tổng hợp và báo cáo đơn vị cơ quan quản lý nhà nước trong trường hợp cần thiết.

2. Khi xảy ra sự cố an toàn thông tin mạng thuộc loại hình tấn công mạng thực hiện báo cáo theo quy định tại Điều 11 Quyết định số 05/2017/QĐ-TTg và Điều 9 Thông tư 20/2017/TT- BTTT. Trách nhiệm của các đơn vị khi phát hiện, tiếp nhận xác minh, xử lý ban đầu và phân loại sự cố an toàn thông tin mạng theo quy định.

3. Quy trình ứng cứu sự cố an toàn thông tin mạng theo quy định tại Điều 13, Điều 14 Quyết định số 05/2017/QĐ-TTg, Điều 11 Thông tư số 20/2017/TT-BTTTT.

Điều 7. Xây dựng, rà soát, cập nhật, bổ sung Quy chế

Định kỳ 02 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.

Điều 8. Bảo đảm nguồn nhân lực

1. Cán bộ chuyên trách được tuyển dụng vào vị trí làm việc về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng.

2. Cán bộ chuyên trách được đảm bảo các điều kiện học tập, tiếp cận công nghệ, kiến thức an toàn bảo mật thông tin trước khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

3. Thường xuyên tổ chức, phổ biến các quy định về đảm bảo an toàn thông tin, nhằm nâng cao nhận thức về trách nhiệm đảm bảo an toàn thông tin cho tổ chức cá nhân sử dụng hệ thống thông tin do đơn vị quản lý.

Điều 9. Thuê khoán dịch vụ công nghệ thông tin

1. Có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc thuê khoán dịch vụ công nghệ thông tin.

2. Nhà phát triển phải cam kết cung cấp các bản vá lỗi bảo mật và bản cập nhật kịp thời khi có phát hiện lỗ hổng hoặc lỗi phát sinh từ phần mềm.

3. Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng:

a. Trước khi đưa hệ thống vào vận hành, tất cả các thành phần phần mềm, phần cứng và các kết nối mạng phải trải qua quá trình kiểm thử toàn diện để đảm bảo tính ổn định và an toàn.

b. Quy trình kiểm thử phải được lập kế hoạch chi tiết, bao gồm phạm vi kiểm thử, công cụ và phương pháp kiểm thử được sử dụng (kiểm thử chức năng, kiểm thử bảo mật, kiểm thử tốc độ tải, …)

c. Ngoài việc kiểm thử trước khi đưa vào sử dụng, hệ thống cũng cần được kiểm thử định kỳ, đặc biệt là sau các bản cập nhật phần mềm hoặc thay đổi cấu trúc.

d. Cán bộ chuyên trách về An toàn hệ thống thông tin có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống, chịu trách nhiệm đảm bảo rằng hệ thống được triển khai một cách an toàn, bảo mật, và đáp ứng các yêu cầu pháp lý và tiêu chuẩn an toàn thông tin, từ giai đoạn thử nghiệm cho đến khi hệ thống được đưa vào sử dụng chính thức.

Điều 10. Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin

Ngắt kết nối hệ thống, sao lưu dữ liệu trước khi gỡ bỏ nếu cần, phải xoá dữ liệu, ghi đè dữ liệu, định dạng ổ cứng trên thiết bị theo quy định bảo mật. Một số trường hợp đặc biệt có thể cần phải phá huỷ vật lý thiết bị/vật lưu trữ trước khi bỏ đi.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 11. Trách nhiệm của các phòng, trạm

1. Lãnh đạo các phòng, trạm thuộc Trung tâm có trách nhiệm tổ chức thực hiện, phổ biến, triển khai Quy chế này đến toàn thể viên chức và người lao động chịu trách nhiệm trước Lãnh đạo Trung tâm trong công tác bảo vệ an toàn, an ninh thông tin của cơ quan, đơn vị mình.

2. Khi có sự cố hoặc nguy cơ mất an toàn thông tin phải kịp thời phối hợp với Phòng Thông tin – Thống kê áp dụng mọi biện pháp để khắc phục và hạn chế thiệt hại, ưu tiên sử dụng lực lượng kỹ thuật an toàn, an ninh thông tin của cơ quan và lập biên bản, báo cáo bằng văn bản cho cơ quan cấp trên quản lý trực tiếp.

3. Phối hợp chặt chẽ với cơ quan Công an trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin. Tạo điều kiện thuận lợi cho các cơ quan chức năng tham gia khắc phục sự cố và thực hiện đúng theo hướng dẫn.

4. Phòng Thông tin và Thống kê hàng năm cử cán bộ tham gia các lớp đào tạo, tập huấn về công tác bảo đảm an toàn thông tin mạng do cơ quan cấp trên tổ chức và tuyên truyền về an toàn thông tin mạng trong công tác quản lý nhà nước trên địa bàn tỉnh.

5. Tổ chức thực hiện, kiểm tra định kỳ hoặc đột xuất về công tác đảm bảo an toàn thông tin mạng, an ninh mạng trong phạm vi quản lý của phòng, trạm. Kịp thời phát hiện và khắc phục những thiếu sót, sơ hở về công tác đảm bảo an toàn thông tin mạng, an ninh mạng trong từng phòng/trạm. Chủ động xây dựng dự toán kinh phí phục vụ công tác đảm bảo an toàn thông tin mạng, an ninh mạng theo quy định hiện hành.

Điều 12. Trách nhiệm của viên chức, lao động hợp đồng

1. Trách nhiệm của cán bộ chuyên trách an toàn an ninh thông tin

a. Chịu trách nhiệm triển khai các biện pháp quản lý vận hành, quản lý kỹ thuật, tham mưu xây dựng các quy định đảm bảo an toàn, an ninh thông tin cho Hệ thống thông tin của Trung tâm theo Quy chế này.

b. Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn, an ninh thông tin.

2. Trách nhiệm của viên chức, lao động hợp đồng

a. Nghiêm chỉnh thi hành các quy chế nội bộ, quy trình về an toàn, an ninh thông tin của Trung tâm cũng như các quy định khác của pháp luật, nâng cao ý thức cảnh giác và trách nhiệm đảm bảo an toàn thông tin, an ninh mạng tại Trung tâm.

b. Khi phát hiện sự cố phải báo cáo ngay với cấp trên và bộ phận chuyên trách để kịp thời ngăn chặn, xử lý.

c. Thực hiện các biện pháp đảm bảo an toàn thông tin mạng, an ninh mạng.

d. Sử dụng thông tin, dữ liệu đúng mục đích, đúng quy định.

Chương IV

TỔ CHỨC THỰC HIỆN

Điều 13. Tổ chức thực hiện Quy chế

1. Trưởng các phòng/trạm, Lãnh đạo Trung tâm có trách nhiệm tổ chức thực hiện Quy chế này.

2. Quy chế này có hiệu lực kể từ ngày ban hành. Trong quá trình thực hiện nếu có những vấn đề vướng mắc, phát sinh thì phản ánh về phòng Thông tin – Thống kê để kịp thời báo cáo Lãnh đạo Trung tâm, đề nghị bổ sung Quy chế cho phù hợp với tình hình thực tế./.