SỞ NÔNG NGHIỆP VÀ PTNT
THÀNH PHỐ HỒ CHÍ MINH
CHI CỤC CHĂN NUÔI VÀ THÚ Y

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

Số: 189 /QĐ-CNTY

Thành phố Hồ Chí Minh, ngày 28 tháng 10 năm 2024

QUYẾT ĐỊNH
Phê duyệt đề xuất cấp độ và phương án bảo đảm an toàn thông tin cho hệ thống thông tin của Chi cục Chăn nuôi và Thú y

CHI CỤC TRƯỞNG CHI CỤC CHĂN NUÔI VÀ THÚ Y

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 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

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

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 Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 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 Quyết định số 1622/QĐ-TTg ngày 25 tháng 10 năm 2017 của Thủ tướng Chính phủ về việc phê duyệt Đề án đẩy mạnh hoạt động của mạng lưới ứng cứu sự cố, tăng cường năng lực cho cán bộ, bộ phận chuyên trách ứng cứu sự cố an toàn thông tin mạng trên toàn quốc đến 2020, định hướng đến 2025;

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 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 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 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 tháng 11 năm 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 tháng 8 năm 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 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 4892/QĐ-UB ngày 13 tháng 9 năm 2017 của Ủy ban nhân dân Thành phố Hồ Chí Minh về tổ chức lại Chi cục Thú y thành Chi cục Chăn nuôi và Thú y trực thuộc Sở Nông nghiệp và Phát triển nông thôn;

Căn cứ Quyết định số 187/QĐ-CNTY ngày 23 tháng 10 năm 2024 về ban hành Quy chế bảo đảm an toàn thông tin, an ninh mạng của Chi cục Chăn nuôi và Thú y;

Theo đề nghị của Trưởng phòng Phòng Tài chính - Tổng hợp.

QUYẾT ĐỊNH:

Điều 1. Phê duyệt cấp độ và phương án bảo đảm an toàn thông tin cho hệ thống thông tin "Hệ thống cơ sở hạ tầng công nghệ thông tin thuộc phạm vi quản lý của Chi cục Chăn nuôi và Thú y, cụ thể như sau:

1. Thông tin chung

a) Tên hệ thống thông tin: Hệ thống cơ sở hạ tầng công nghệ thông tin thuộc phạm vi quản lý của Chi cục Chăn nuôi và Thú y.

Bao gồm 02 hệ thống thông tin thành phần:

- Hệ thống cơ sở hạ tầng công nghệ thông tin tại Văn phòng Chi cục Chăn nuôi và Thú y, số 151 Lý Thường Kiệt, Phường 7, Quận 11, TP. Hồ Chí Minh; điện thoại: 028.38536132

- Hệ thống cơ sở hạ tầng công nghệ thông tin tại các Trạm trực thuộc Chi cục (theo Phụ lục 1: Danh sách các Trạm trực thuộc đính kèm).

b) Đơn vị vận hành hệ thống thông tin: Bộ phận công nghệ thông tin của Phòng Tài chính - Tổng hợp Chi cục Chăn nuôi và Thú y.

2. Cấp độ an toàn hệ thống thông tin: **Cấp độ 2**

3. Phương án bảo đảm an toàn thông tin trong thiết kế, quá trình vận hành hệ thống thông tin tương ứng với cấp độ 2 phù hợp với quy định tại Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 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 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

(Thuyết minh Phương án Ứng cứu sự cố đảm bảo an toàn thông tin, an ninh mạng tại Chi cục Chăn nuôi và Thú y; Phụ lục ban hành kèm theo Quyết định này).

Điều 2. Tổ chức thực hiện

1. Bộ phận công nghệ thông tin của Phòng Tài chính - Tổng hợp, có trách nhiệm bảo đảm an toàn hệ thống thông tin theo các quy định tại Điều 22 Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Các phòng, trạm trực thuộc khi triển khai các hệ thống thông tin trên hạ tầng của Hệ thống cơ sở hạ tầng công nghệ thông tin thuộc phạm vi quản lý của Chi cục Chăn nuôi và Thú y phải tuân thủ các phương án bảo đảm an toàn đã được phê duyệt.

3. Bộ phận công nghệ thông tin của Phòng Tài chính - Tổng hợp, có trách nhiệm kiểm tra, giám sát thực hiện, báo cáo Lãnh đạo Chi cục và các cấp thẩm quyền theo quy định của pháp luật.

Điều 3. Trưởng phòng Phòng Tài chính - Tổng hợp, Trưởng các phòng, trạm trực thuộc Chi cục và các đơn vị có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Sở NN và PTNT;
- Sở Thông tin và Truyền thông;
- Ban Lãnh đạo Chi cục;
- Lưu: VT, TCTH (06).

CHI CỤC TRƯỞNG

SỞ NÔNG NGHIỆP VÀ PHÁT TRIỂN NÔNG THÔN T.P CẦN THƠ
CHI CỤC CHĂN NUÔI VÀ THÚ Y

Lê Việt Bảo

Phụ lục

DANH SÁCH CÁC TRẠM TRỰC THUỘC

(Kèm theo Quyết định số 189/QĐ-CNTY ngày 28 tháng 10 năm 2024 của Chi cục Chăn nuôi và Thú y)

STT	Đơn vị	Điện thoại	Địa chỉ
1	Trạm CNTY Liên quận 3-10-11	028.39274 625	462 Lý Thái Tổ, Phường 10, Quận 11 Email: cnty31011@chicuccntyhcm.gov.vn
2	Trạm CNTY Liên quận 1-4-7	028.39201 141	178 Trần Hưng Đạo, phường Nguyễn Cư Trinh, Quận 1 Email: cnty147@chicuccntyhcm.gov.vn
3	Trạm CNTY Liên quận 5-6-8	028.39235 717	1091 Trần Hưng Đạo, Phường 5, Quận 5 Email: cnty568@chicuccntyhcm.gov.vn
4	Trạm CNTY Liên quận 12-GV	028.35880 342	30 Nguyễn Văn Nghi, Phường 5, quận Gò Vấp Email: cnty12gv@chicuccntyhcm.gov.vn
5	Trạm CNTY Liên quận Phú Nhuận, Bình Thạnh	028.38991 993	313 Xô Viết Nghệ Tĩnh, Phường 24, quận Bình Thạnh Email: cntypnbth@chicuccntyhcm.gov.vn
6	Trạm CNTY Liên quận Tân Bình, Tân Phú, Bình Tân	028.39770 592	1009 Cách Mạng Tháng Tám, Phường 7 quận Tân Bình Email: cntytbtpbta@chicuccntyhcm.gov.vn
7	Trạm CNTY Cần Giờ	028.38740 044	Số 2, dãy 12 căn, thị trấn Cần Thạnh, huyện Cần Giờ Email: cntycangio@chicuccntyhcm.gov.vn
8	Trạm CNTY Nhà Bè	028.37800 433	308D Nguyễn Văn Tạo, xã Long Thới, huyện Nhà Bè Email: cntynhabe@chicuccntyhcm.gov.vn
9	Trạm CNTY Bình Chánh	028.37604 659	E4/19A Nguyễn Hữu Trí, thị trấn Tân Túc, huyện Bình Chánh Email:cntybinhchanh@chicuccntyhcm.gov.vn
10	Trạm CNTY thành phố Thủ Đức	028.38972 935	330 Võ Văn Ngân, phường Bình Thọ, thành phố Thủ Đức Email: cnty29td@chicuccntyhcm.gov.vn
11	Trạm CNTY Củ Chi	028.38921 364	Nguyễn Văn On, khu phố 2, thị trấn Củ chi, huyện Củ chi Email: cntycuchi@chicuccntyhcm.gov.vn
12	Trạm CNTY Hóc Môn	028.38834 506	161/5A Quốc lộ 22, ấp Trung Chánh 2, xã Trung Chánh, huyện Hóc Môn Email: cntyhocmon@chicuccntyhcm.gov.vn

13	Trạm KDĐV Hóc Môn	028.37180 626	ấp 21, xã Tân Thới Nhì, huyện Hóc Môn Email: kddvhocmon@chicuccntyhcm.gov.vn
14	Trạm KDĐV An Lạc	028.37606 196	B5/1 Quốc lộ 1A, xã Bình Chánh, huyện Bình Chánh Email: kddvanlac@chicuccntyhcm.gov.vn
15	Trạm KDĐV Thủ Đức	028.37251 197	Km 18 Xa lộ Hà Nội, phường Linh Trung, thành phố Thủ Đức Email: kddvthuduc@chicuccntyhcm.gov.vn
16	Trạm KDĐV Xuân Hiệp	028.38975 224	249/1 Quốc lộ 1K, phường Linh Xuân, thành phố Thủ Đức Email:kddvxuanhiep@chicuccntyhcm.gov.vn
17	Trạm Chẩn đoán xét nghiệm và Điều trị bệnh động vật	028.39555 623	128 Trần Quý, Phường 6, Quận 11 Email: cdxn@chicuccntyhcm.gov.vn

SỞ NÔNG NGHIỆP VÀ PTNT
THÀNH PHỐ HỒ CHÍ MINH
CHI CỤC CHĂN NUÔI VÀ THÚ Y

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

PHƯƠNG ÁN
Ứng cứu sự cố đảm bảo an toàn thông tin, an ninh mạng tại Chi cục Chăn nuôi và Thú y

(Kèm theo Quyết định số 189 /QĐ-CNTY ngày 28 tháng 10 năm 2024 của Chi cục Chăn nuôi và Thú y)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi áp dụng

Phương án này quy định việc phối hợp ứng phó sự cố mất an toàn thông tin (ATTT), an ninh mạng trong hoạt động ứng dụng công nghệ thông tin của các phòng trạm trực thuộc Chi cục Chăn nuôi và Thú y.

Điều 2. Đối tượng áp dụng

1. Các phòng, trạm trực thuộc Chi cục.

2. Công chức, viên chức, người lao động (CCVC-LĐ) của các phòng, trạm trực thuộc và các tổ chức, cá nhân khác liên quan.

Điều 3. Nguyên tắc, phương châm ứng phó sự cố

Sự cố mất an toàn thông tin, hệ thống thông tin cần ứng phó khi xảy ra một trong các trường hợp sau:

- Hệ thống mạng nội bộ và mạng internet bị gián đoạn dịch vụ.

- Dữ liệu bí mật nhà nước có khả năng bị tiết lộ.

- Dữ liệu quan trọng của hệ thống không đảm bảo tính toàn vẹn và không có khả năng khôi phục được.

- Hệ thống bị mất quyền điều khiển.

- Sự cố có khả năng xảy ra trên diện rộng hoặc gây ra ảnh hưởng mang tính dây chuyền.

- Bộ phận quản trị hệ thống thông tin không đủ khả năng kiểm soát, xử lý được xự cố.

Điều 4. Chức năng, nhiệm vụ, trách nhiệm và cơ chế, quy trình phối hợp giữa các lực lượng tham gia ứng cứu sự cố

- Bộ phận công nghệ thông tin của Phòng Tài chính - Tổng hợp là bộ phận đầu mối, chủ trì phối hợp cùng Sở Nông nghiệp và phát triển nông thôn, Sở Thông tin Truyền thông và Đội ứng cứu sự cố an toàn thông tin mạng của Thành

phố có trách nhiệm tham gia hoạt động ứng cứu khẩn cấp đảm bảo ATTT, an ninh mạng của Chi cục đảm bảo duy trì hoạt động công vụ xuyên suốt.

- Các phòng trạm trực thuộc Chi cục có trách nhiệm phân công nhân sự phụ trách ATTT, an ninh mạng tham gia ứng cứu cùng với Bộ phận công nghệ thông tin của Phòng Tài chính - Tổng hợp khi xảy ra sự cố ATTT, an ninh mạng.

Chương II

ĐÁNH GIÁ CÁC NGUY CƠ, SỰ CỐ AN TOÀN THÔNG TIN

Điều 5. Đánh giá các nguy cơ, sự cố an toàn thông tin, an ninh mạng

Định kỳ hàng quý, Bộ phận công nghệ thông tin của Phòng Tài chính - Tổng hợp thực hiện đánh giá các nguy cơ, sự cố như sau:

a) Đánh giá hiện trạng và khả năng đảm bảo ATTT, an ninh mạng của các hệ thống thông tin và các đối tượng cần bảo vệ.

b) Đánh giá, dự báo nguy cơ, sự cố, tấn công mạng có thể xảy ra với các hệ thống thông tin và các đối tượng cần bảo vệ.

c) Đánh giá, dự báo các hậu quả, thiệt hại, tác động có thể có nếu xảy ra sự cố mất ATTT, an ninh mạng.

d) Đánh giá về hiện trạng phương tiện, trang thiết bị, công cụ hỗ trợ, nhân lực, vật lực phục vụ đối phó, ứng cứu, khắc phục sự cố *(bao gồm cả nhà thầu đã ký hợp đồng cung cấp dịch vụ nếu có).*

Điều 6. Tiêu chí xây dựng phương án đối phó, ứng cứu sự cố mất an toàn thông tin, an ninh mạng

Phương án đối phó, ứng cứu sự cố ATTT, an ninh mạng phải đề ra các tiêu chí để có thể nhanh chóng xác định được tính chất, mức độ nghiêm trọng của sự cố khi sự cố xảy ra. Việc xây dựng phương án đối phó, ứng cứu sự cố ATTT, an ninh mạng cần đảm bảo các nội dung sau:

- Phương pháp, cách thức để xác định nhanh chóng, kịp thời nguyên nhân, nguồn gốc sự cố nhằm áp dụng phương án đối phó, ứng cứu, khắc phục sự cố phù hợp.

- Sự cố do bị tấn công mạng từ tác động bên ngoài.

- Sự cố do lỗi hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường điện, đường truyền, hosting, …

- Sự cố do lỗi của người quản trị, vận hành hệ thống.

- Sự cố liên quan đến các thảm họa tự nhiên thiên tai như bão, lụt, động đất, hỏa hoạn.

Chương III

PHƯƠNG ÁN ỨNG CỨU SỰ CỐ ÁP DỤNG ĐỐI VỚI MỘT SỐ TÌNH HUỐNG

Điều 7. Phương án đối phó, ứng cứu, khắc phục sự cố đối với một hoặc nhiều tình huống

1. Sự cố do bị tấn công mạng

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

2. Tình huống sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật

- Sự cố nguồn điện.
- Sự cố đường kết nối mạng internet.
- Sự cố do lỗi phần mềm, phần cứng, ứng dụng của hệ thống thông tin.
- Sự cố liên quan đến quá tải hệ thống.
- Sự cố khác do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật.

3. Tình huống sự cố do lỗi của người quản trị, vận hành hệ thống

- Lỗi trong cập nhật, thay đổi, cấu hình phần cứng.
- Lỗi trong cập nhật, thay đổi, cấu hình phần mềm.
- Lỗi liên quan đến chính sách và thủ tục an toàn thông tin.
- Lỗi liên quan đến việc dừng dịch vụ vì lý do bắt buộc.
- Lỗi khác liên quan đến người quản trị, vận hành hệ thống.

4. Tình huống sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn, …

Công tác tổ chức, điều hành, phối hợp giữa các lực lượng, giữa các tổ chức trong đối phó, ngăn chặn, ứng cứu, khắc phục sự cố và theo sự phân công của Lãnh đạo, chỉ đạo của Ủy ban nhân dân Thành phố, Sở Nông nghiệp và Phát triển nông thôn.

Chương IV
TRIỂN KHAI CÁC GIẢI PHÁP PHÒNG NGỪA SỰ CỐ, GIÁM SÁT PHÁT HIỆN, ĐẢM BẢO CÁC ĐIỀU KIỆN SẴN SÀNG ỨNG PHÓ KHẮC PHỤC SỰ CỐ

Điều 8. Các nội dung, nhiệm vụ cụ thể cần triển khai nhằm phòng ngừa sự cố, đảm bảo các điều kiện sẵn sàng ứng phó, khắc phục sự cố

1. Các nội dung nhằm phát hiện sớm và phòng ngừa sự cố

a) Thực hiện nghiêm công tác giám sát, phát hiện sớm nguy cơ sụp đổ.

b) Kiểm tra, đánh giá ATTT, an ninh mạng và rà quét, bóc gỡ, phân tích, xử lý mã độc.

c) Phòng ngừa sự cố, quản lý rủi ro; nghiên cứu, phân tích, xác minh, cảnh báo sự cố, rủi ro ATTT, an ninh mạng, phần mềm độc hại.

d) Cần phải xây dựng thêm quy trình, quy định, tiêu chuẩn về ATTT, an ninh mạng; tuyên truyền, nâng cao nhận thức về nguy cơ, sự cố tấn công mạng.

2. Các nội dung nhằm đảm bảo các điều kiện sẵn sàng ứng phó, khắc phục sự cố

a) Trang bị, nâng cấp thiết bị, công cụ, phương tiện, gia hạn bản quyền phần mềm phục vụ việc ứng cứu, khắc phục sự cố.

b) Thuê dịch vụ đảm bảo ATTT, an ninh mạng, chuẩn bị các nguồn lực sẵn sàng để ứng phó, khắc phục khi sự cố xả ra.

c) Tham gia các lớp tập huấn, các hoạt động của mạng lưới ứng cứu sự cố.

d) Phối hợp chặt chẽ với Sở Nông nghiệp và Phát triển nông thôn, Sở Thông tin và Truyền Thông, Đội ứng cứu sự cố an toàn thông tin mạng của Thành phố khi có tình huống xảy ra.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 9. Trách nhiệm của Phòng Tài chính tổng hợp

- Là đơn vị chủ trì, phối hợp với các phòng trạm trực thuộc Chi cục triển khai thực hiện các nội dung tại phương án này.

- Là đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về ATTT, an ninh mạng trong hoạt động của Chi cục.

- Bộ phận công nghệ thông tin của Phòng Tài chính - Tổng hợp chủ động cài đặt phần mềm diệt virus, tường lửa cho hệ thống máy tính, hệ thống mạng, hệ thống thông tin tại các phòng, trạm trực thuộc Chi cục.

- Chủ trì, phối hợp với các phòng, trạm trực thuộc Chi cục tiến hành kiểm tra công tác đảm bảo ATTT, an ninh mạng định kỳ hàng năm hoặc theo hướng dẫn của cơ quan thẩm quyền quản lý về chuyên môn.

- Tham mưu đưa nội dung dự toán kinh phí, nhân lực, vật lực thường trực sẵn sàng ứng cứu sự cố; triển khai điều hành, phối hợp tổ chức ứng cứu và thực hiện ứng cứu, xử lý, ngăn chặn, khắc phục sự cố vào các kế hoạch về đảm bảo ATTT, an ninh mạng, kế hoạch ứng dụng công nghệ thông tin hàng năm trong công tác chỉ đạo điều hành của Chi cục.

Điều 10. Trách nhiệm của các phòng trạm trực thuộc

- Quan tâm, chú trọng đến công tác đảm bảo ATTT, an ninh mạng cho hệ thống thông tin được giao quản lý.

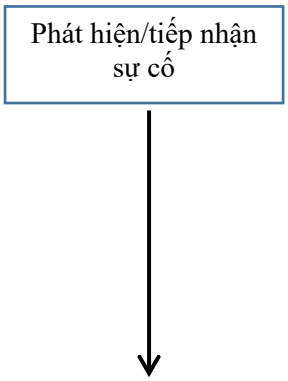
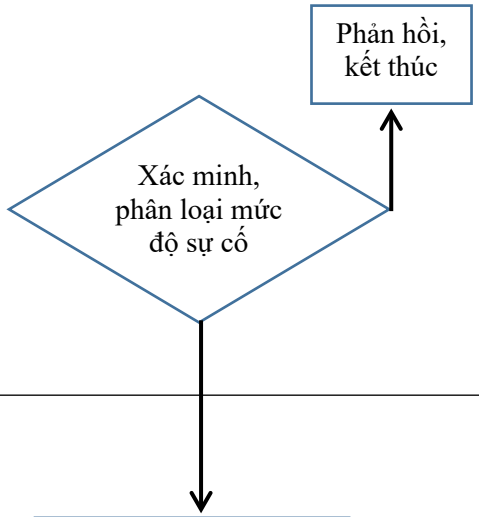
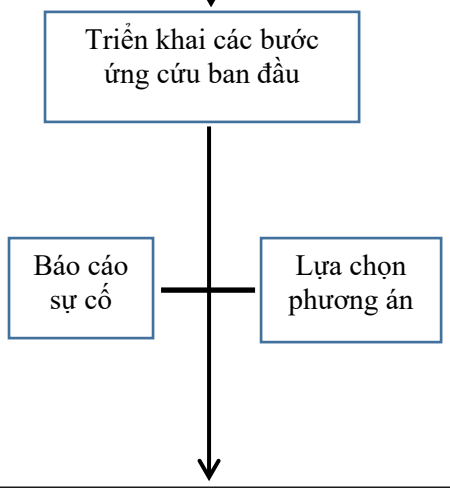
- Các phòng, trạm trực thuộc chủ động phối hợp với Bộ phận công nghệ thông tin của Phòng Tài chính - Tổng hợp và các đơn vị liên quan thực hiện công tác ứng phó sự cố ATTT, an ninh mạng thuộc phạm vi quản lý.

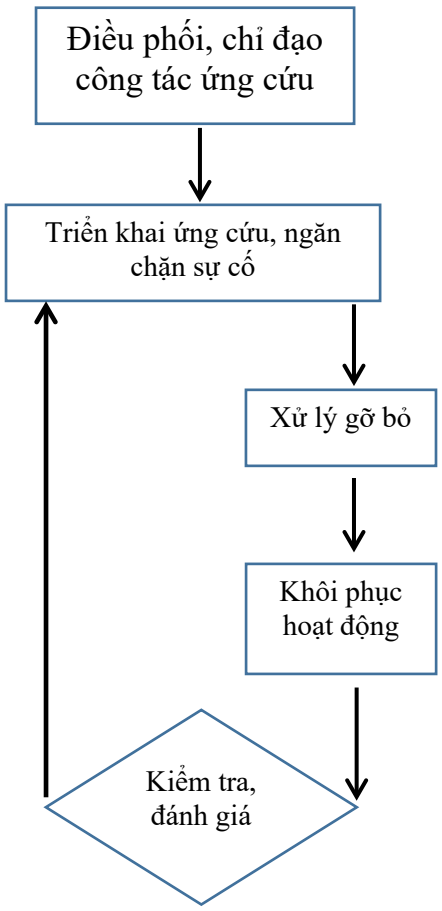
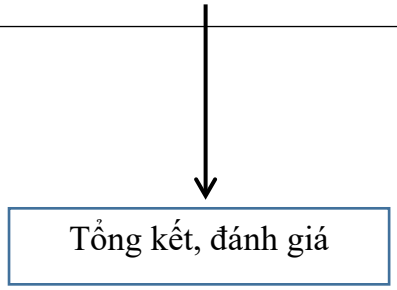
- Trong quá trình thực hiện nhiệm vụ, CCVC-LĐ tuyệt đối không truy cập các website không đảm bảo an toàn, không truy xuất các đường link lạ được gửi qua hộp thư điện tử công vụ, nếu có các hộp thư điện tử chứa đường dẫn lạ trong hộp thư điện tử thì liên hệ với Bộ phận công nghệ thông tin của Phòng Tài chính - Tổng hợp kiểm tra, xem xét và hướng dẫn trước khi truy cập.

Trên đây là Phương án ứng cứu sự cố đảm bảo ATTT, an minh mạng tại Chi cục Chăn nuôi và Thú y, trong quá trình triển khai thực hiện nếu có vấn đề phát sinh, vướng mắc, kịp thời phản ánh thông tin về Phòng Tài chính - Tổng hợp để báo cáo Ban Lãnh đạo Chi cục xem xét, sửa đổi, bổ sung phù hợp với tình hình thực tế./.

CHI CỤC CHĂN NUÔI VÀ THÚ Y

Phụ lục 1: Quy trình ứng cứu sự cố an toàn thông tin mạng

Thành phần	Tiến trình	Quy trình	Ghi chú
- Sở Nông nghiệp và PTNT - Sở Thông tin và Truyền thông - Chi cục Chăn nuôi và Thú y và các phòng, trạm trực thuộc Chi cục.	Bước 1		Thông tin sự cố có thể từ các nguồn: Đội Ứng cứu sự cố của Thành phố - Sở Nông nghiệp và PTNT - Sở Thông tin và Truyền thông - Phòng, trạm trực thuộc Chi cục - Thông tin từ xã hội
- Chi cục CNTY và các phòng, trạm trực thuộc Chi cục (cán bộ được phân công).	Bước 2		- Chuyên viên quản trị mạng của Chi cục và các phòng, trạm trực thuộc Chi cục xác minh ban đầu sự cố, phân loại sự cố và mức độ sự cố (Thông thường hay nghiêm trọng). Báo cáo phản hồi (Nếu không ảnh hưởng thì Báo cáo kết thúc).
- Chuyên viên quản trị mạng Chi cục và các phòng, trạm trực thuộc Chi cục (cán bộ được phân công) - Đội ứng cứu sự cố ATTT của Thành phố, Sở Nông nghiệp và PTNT, Sở Thông tin và Truyền thông	Bước 3		- Chuyên viên quản trị mạng của Chi cục và các đơn vị trực thuộc Chi cục triển khai các bước ứng cứu ban đầu, lựa chọn phương án ứng cứu tiếp theo đồng thời báo cáo sự cố cho BLĐ Chi cục và các đơn vị chuyên trách Ứng cứu sự cố. - Đội ứng cứu sự cố ATTT của Thành phố, Bộ phận quản trị mạng của Sở Nông nghiệp và PTNT, Sở Thông tin và Truyền thông hỗ trợ

- Chuyên viên quản trị mạng Chi cục và các phòng, trạm trực thuộc Chi cục (cán bộ được phân công) - Đội ứng cứu sự cố ATTT của Thành phố, Sở Nông nghiệp và và PTNT, Sở Thông tin và Truyền thông	Bước 4		- Sự cố thông thường: Chuyên viên quản trị mạng Chi cục và các phòng, trạm trực thuộc Chi cục triển khai phương án đối phó, ứng cứu một số tình huống cụ thể hoặc theo hướng dẫn của đội ứng cứu sự cố ATTT của Thành phố, Sở Nông nghiệp và PTNT, Sở Thông tin và Truyền thông. - Sự cố nghiêm trọng: Báo cáo và phối hợp với Đội ứng cứu sự cố của Thành phố, Sở Nông nghiệp và PTNT, Sở Thông tin và Truyền thông trong công tác ứng cứu sự cố an toàn thông tin mạng tại đơn vị. - Khi kiểm tra, đánh giá nếu hệ thống chưa hoạt động bình thường thì quay lại tiếp tục công tác ứng cứu sự cố.
- Chuyên viên quản trị mạng Chi cục và các phòng, trạm trực thuộc Chi cục (cán bộ được phân công). - Đội ứng cứu sự cố ATTT của Thành phố, Sở Nông nghiệp và PTNT, Sở Thông tin và Truyền thông	Bước 5		- Đối với sự cố thông thường: Cần thực hiện việc tổng kết, đánh giá ứng cứu sự cố và có các báo cáo cho các cấp liên quan. - Đối với sự cố nghiêm trọng: Cần phải thực hiện việc tổng hợp, báo cáo sự cố cho các cấp có thẩm quyền, chia sẻ thông tin trong mạng lưới ứng cứu, công bố chính thức với xã hội và truyền thông.

Phụ lục 2: Phương án đối phó, ứng cứu một số tình huống cụ thể

1. Sự cố gây rò rỉ dữ liệu

Tiến trình	Nội dung tham khảo thực hiện
Dấu hiệu	- Dữ liệu của Chi cục, phòng, trạm trực thuộc bị rò rỉ, phát tán trên không gian mạng. - Tài khoản truy cập vào các hệ thống phần mềm dùng chung bị chiếm đoạt, khai thác trái phép. - Dữ liệu bị thay đổi, xóa bỏ, lấy cắp trái phép.
Xử lý ưu tiên, ban đầu	- Đối với Chi cục: Chuyên viên quản trị mạng của Chi cục cùng với đơn vị vận hành hệ thống thuê ngoài (nếu có) báo cáo Lãnh đạo Chi cục và liên hệ Đội Ứng cứu sự cố an toàn thông tin mạng của Thành phố. - Đối với các phòng, trạm trực thuộc: báo thông tin về Bộ phận CNTT của Phòng Tài chính - Tổng hợp Chi cục để phối hợp cùng Đội ứng cứu sự cố an toàn thông tin mạng của Thành phố. - Ưu tiên cô lập hệ thống: Tách máy tính, thiết bị nghi ngờ rò rỉ dữ liệu ra khỏi hệ thống mạng nội bộ và ngắt kết nối Internet. - Tiến hành xác minh nhanh dữ liệu bị rò rỉ, xác định mức độ và phạm vi rò rỉ dữ liệu.
Xác định nguyên nhân, đánh giá tác động của sự cố và xử lý ban đầu	- Từ những dấu hiệu, thông tin thu được khoanh vùng nguyên nhân, nguồn gốc ban đầu của cuộc tấn công. - Thông báo với các đơn vị liên quan mức độ, phạm vi ảnh hưởng ban đầu và thời gian dự kiến khắc phục của sự cố. - Đánh giá sơ bộ về thiệt hại hoặc mức độ ảnh hưởng của sự cố.
Cô lập hệ thống	- Thực hiện cô lập hệ thống bị tấn công để tránh bị thay đổi hiện trường. - Thông báo tới các cơ quan chức năng và đối tác để hỗ trợ.
Xử lý sự cố	- Xác định nguyên nhân của sự cố an ninh mạng. - Rà soát hệ thống để phát hiện các lỗ hổng có thể bị khai thác tấn công vào cơ sở dữ liệu. - Rà soát khả năng lộ mật khẩu của các tài khoản quản trị, tài khoản có quyền quản trị cơ sở dữ liệu. - Rà quét và xử lý mã độc trên máy tính của người sử dụng các tài khoản này, thay đổi mật khẩu các tài khoản.

Khôi phục hệ thống	- Xác định được lỗ hổng mà hacker đã sử dụng để tấn công, vá các lỗ hổng này. - Rà soát và vá các lỗ hổng ở module khác của hệ thống. - Sử dụng các công cụ rà quét mạng để phát hiện bất kỳ truy cập nào trái phép hoặc phát hiện sự quay trở lại của hacker.
Tổng kết, đánh giá	- Điều tra chi tiết hơn về sự cố để mở rộng phạm vi và chống các ảnh hưởng tiềm tàng khác. - Tông hợp lại toàn bộ các thông tin liên quan đến sự cố, đánh giá, xử lý sự cố và khôi phục hệ thống để làm tài liệu tham khảo cho các lần sau. - Phối hợp các cơ quan chức năng để phối hợp mở rộng phạm vi

2. Sự cố tấn công thay đổi giao diện

Tiến trình	Nội dung tham khảo thực hiện
Dấu hiệu	Trang thông tin điện tử của Chi cục bị thay đổi trái phép nội dung toàn bộ hoặc một phần.
Xử lý ưu tiên, ban đầu	- Ưu tiên cô lập hệ thống cung cấp dịch vụ Website. - Kích hoạt hệ thống dự phòng hoặc trang thông báo lỗi, bảo trì.
Xác định nguyên nhân, đánh giá tác động của sự cố và xử lý ban đầu	- Từ những dấu hiệu, thông tin thu được khoanh vùng nguyên nhân, nguồn gốc ban đầu của cuộc tấn công. - Kiểm tra xem tên miền có trỏ đúng vào máy chủ web hay không, liên hệ với đơn vị quản lý tên miền để xác định trạng thái tài khoản quản lý tên miền. - Trong trường hợp tên miền không bị chiếm quyền điều khiển: Thực hiện thay thế nội dung trang chủ bằng thông báo bảo trì, nâng cấp hệ thống. - Trong trường hợp tên miền bị chiếm quyền điều khiển: + Yêu cầu lấy lại quyền điều khiển tên miền. + Cấu hình tên miền trỏ đúng về địa chỉ máy chủ web. + Yêu cầu khóa tài khoản quản lý tên miền này, không cho phép cập nhật các thông tin liên quan. -Thông báo với các đơn vị liên quan mức độ, phạm vi ảnh hưởng ban đầu và thời gian dự kiến khắc phục của sự cố.

Cô lập hệ thống và kích hoạt hoạt động hệ thống dự phòng	- Thực hiện cô lập hệ thống bị tấn công để tránh bị thay đổi hiện trường. - Rà soát khả năng bị tấn công khai thác của hệ thống dự phòng và chuyển đổi sang hệ thống dự phòng. - Trong trường hợp hệ thống dự phòng cũng bị tấn công, thực hiện trỏ tên miền tới trang thông tin điện tử của Sở Nông nghiệp và PTNT, đồng thời thực hiện xây dựng hệ thống mới. - Tạm ngắt các tài khoản quản trị, tài khoản có quyền đăng bài lên website. - Thông báo Đội Ứng cứu sự cố an toàn thông tin mạng của Thành phố để hỗ trợ.
Xử lý sự cố	- Xác định nguyên nhân của sự cố an ninh mạng. - Điều tra, phân tích hệ thống để tìm kiếm các shell, file lạ, phân tích hành vi và xác định nguyên nhân của cuộc tấn công. - Thu thập tất cả các thành phần file độc hại và phối hợp với các đối tác phân tích, điều tra. - Phân tích các hành vi của shell và mã độc. - Xác định và xử lý được đầy đủ các thành phần của mã độc. + File shell hacker đã tải lên server. + Tiến trình của mã độc, file của mã độc. + Thành phần đăng ký khởi động cùng server của mã độc - Rà soát khả năng lộ mật khẩu của các user quản trị, user có quyền đăng bài lên website. - Rà quét và xử lý mã độc trên máy tính của user này, sau đó đổi mật khẩu các user.
Khôi phục hệ thống	- Xác định được lỗ hổng mà hacker đã sử dụng để tấn công, vá các lỗ hổng này. - Rà soát và vá các lỗ hổng ở module khác của hệ thống. - Sử dụng các công cụ rà quét mạng để phát hiện bất kỳ truy cập nào trái phép hoặc phát hiện sự quay trở lại của hacker. - Đưa hệ thống chính quay lại hoạt động.

Tổng kết, đánh giá	-Điều tra chi tiết hơn về sự cố để mở rộng phạm vi và chống các ảnh hưởng tiềm tàng khác. -Tổng hợp lại toàn bộ các thông tin liên quan đến sự cố, đánh giá, xử lý sự cố và khôi phục hệ thống để làm tài liệu tham khảo cho các lần sau. -Phối hợp các cơ quan chức năng để phối hợp mở rộng phạm vi.

3. Tấn công mã độc

Tiến trình	Nội dung tham khảo thực hiện
Dấu hiệu	Hệ thống thông tin/máy tính trong Chi cục, phòng, trạm trực thuộc bị tấn công bởi các dạng mã độc khác nhau.
Xử lý ưu tiên, ban đầu	- Đối với Chi cục: Chuyên viên quản trị mạng của Chi cục liên hệ đội Ứng cứu sự cố an toàn thông tin mạng của Thành phố để được hỗ trợ khi cần thiết - Đối với các phòng, trạm trực thuộc: các đơn vị tự xử lý sự cố, khi cần thiết thì báo về Bộ phận CNTT của Phòng Tài chính - Tổng hợp Chi cục để được hỗ trợ. - Ưu tiên cô lập toàn bộ các máy bị lây nhiễm hoặc có dấu hiệu bất thường. - Kiểm tra các máy tính có dữ liệu quan trọng, cô lập và có biện pháp sao lưu dữ liệu.
Xác định nguyên nhân, đánh giá tác động của sự cố và xử lý ban đầu	- Từ những dấu hiệu, thông tin thu được khoanh vùng nguyên nhân, nguồn gốc ban đầu của cuộc tấn công. - Xác định cấu phần thuộc hệ thống bị ảnh hưởng/phạm vi bị ảnh hưởng. - Thông báo với các đơn vị liên quan mức độ, phạm vi ảnh hưởng ban đầu và thời gian dự kiến khắc phục của sự cố.
Cô lập hệ thống	- Thực hiện cô lập hệ thống bị tấn công để tránh bị thay đổi hiện trường và thông báo về khoảng thời gian tạm dừng hệ thống dự kiến. - Thông báo Đội Ứng cứu sự cố an toàn thông tin mạng của Thành phố để hỗ trợ.

Xử lý sự cố	- Xác định nguyên nhân của sự cố an ninh mạng. - Điều tra, phân tích hệ thống để tìm kiếm các shell, file lạ, phân tích hành vi của nó và xác định nguyên nhân của cuộc tấn công. - Thu thập tất cả các thành phần file độc hại và phối hợp với các đối tác phân tích, điều tra. - Phân tích các hành vi của shell và mã độc. - Xác định và xử lý được đầy đủ các thành phần của mã độc *+ File shell hacker đã tải lên server hoặc máy phòng, trạm bị lây nhiễm* *+ Tiến trình của mã độc* *+ File của mã độc* *+ Thành phần đăng ký khởi động của mã độc* - Rà soát khả năng lộ mật khẩu của các tài khoản quản trị, tài khoản có quyền trên hệ thống. - Rà quét và xử lý mã độc trên máy tính của các người dùng sử dụng tài khoản này, thay đổi mật khẩu.
Khôi phục hệ thống	- Xác định được lỗ hổng mà hacker đã sử dụng để tấn công, vá các lỗ hổng này. - Rà soát và vá các lỗ hổng ở module khác của hệ thống. - Thực hiện ngăn chặn mã hash, C&C server (nếu có) trên hệ thống bảo mật tại đơn vị như: Antivirus, Firewall, IPS. - Đưa hệ thống chính quay lại hoạt động. - Sử dụng các công cụ rà quét mạng để phát hiện bất kỳ truy cập nào trái phép hoặc phát hiện sự quay trở lại của hacker.
Tổng kết, đánh giá	-Điều tra chi tiết hơn về sự cố để mở rộng phạm vi và chống các ảnh hưởng tiềm tàng khác. -Tổng hợp lại toàn bộ các thông tin liên quan đến sự cố, đánh giá, xử lý sự cố và khôi phục hệ thống để làm tài liệu tham khảo cho các lần sau. - Phối hợp các cơ quan chức năng để phối hợp mở rộng phạm vi

CHI CỤC CHĂN NUÔI VÀ THÚ Y