UỶ BAN NHÂN DÂN TỈNH TUYÊN QUANG **SỞ NÔNG NGHIỆP VÀ PTNT**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 735/SNN-VP V/v tăng cường đảm bảo an toàn cho hệ thống thông tin	*Tuyên Quang, ngày 08 tháng 5 năm 2019*

Kính gửi: Các đơn vị trực thuộc Sở.

Thực hiện Văn bản số 406/UBND-THCB ngày 25/02/2019 của Uỷ ban nhân dân tỉnh về việc tăng cường đảm bảo an toàn thông tin; Kế hoạch số 94/KH-SNN ngày 24/10/2018 của Sở Nông nghiệp và Phát triển nông thôn về Ứng dụng công nghệ thông tin năm 2019,

Sở Nông nghiệp và Phát triển nông thôn yêu cầu các đơn vị trực thuộc Sở:

1. Thực hiện nghiêm túc các nội dung chỉ đạo của Sở về việc tăng cường công tác đảm bảo an ninh, an toàn thông tin tại Văn bản số 1249/SNN-VP ngày 09/8/2018.

2. Tổ chức triển khai hoạt động tổng kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng cho các hệ thống máy tính, thiết bị mạng, phần cứng, phần mềm hệ thống, phần mềm ứng dụng của cơ quan, đơn vị, nếu phát hiện hoặc nghi ngờ các vấn đề có nguy cơ gây mất an toàn thông tin mạng cần thông báo ngay về Sở *(qua Văn phòng Sở - Đ/c Nguyễn Thị Khánh Vân - chuyên viên CNTT, điện thoại: 0985925896, Email: ntkvannnptnt@tuyenquang.gov.vn)* để được hướng dẫn, hỗ trợ xử lý.

3. Giao Văn phòng Sở là đầu mối tiếp nhận sự cố an toàn thông tin của Sở. Chủ trì phối hợp với các đơn vị tiến hành kiểm tra, rà soát, đánh giá an toàn thông tin mạng khi có yêu cầu hỗ trợ từ các phòng, đơn vị trực thuộc theo quy trình tại Phụ lục 01; kịp thời phát hiện và xử lý sự cố, lỗ hổng, ngăn chặn, bóc gỡ mã độc tấn công vào hệ thống mạng theo quy trình tại Phụ lục 02. Đặc biệt chú trọng phát hiện và xử lý các mã độc có tính chất nguy hiểm, tiềm ẩn sâu bên trong hệ thống máy tính và có khả năng gây rủi ro cao.

Trường hợp sự cố ngoài phạm vi khả năng hỗ trợ phải báo cáo Lãnh đạo Sở xin hỗ trợ từ các cơ quan chuyên trách ứng cứu sự cố của tỉnh hoặc liên hệ

đầu mối thông báo sự cố Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), điện thoại: 02432091616, Email: *ais@mic.gov.vn.*

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Nơi nhận:
- Như kính gửi;
- Văn phòng Sở;
- Lãnh đạo Sở;
- Lưu: VT, VP.

(thực hiện)

CỘNG HOÀ X.H.C.N VIỆT NAM
SỞ NÔNG NGHIỆP VÀ PHÁT TRIỂN NÔNG THÔN
TỈNH TUYÊN QUANG

Nguyễn Công Hàm

Phụ lục 01
QUY TRÌNH KIỂM TRA, RÀ SOÁT, ĐÁNH GIÁ BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

(Kèm theo Công văn số 735 /SNN-VP, ngày 08/5 /2019 của Sở Nông nghiệp và PTNT)

1. Mục đích

Tài liệu này hướng dẫn các hoạt động thực hiện kiểm tra, rà soát, đánh giá đảm bảo an toàn thông tin mạng tại Sở và các đơn vị trực thuộc Sở (sau đây gọi chung là cơ quan, đơn vị) bao gồm: Trang Thông tin điện tử của Sở; hệ thống phần mềm ứng dụng công nghệ thông tin; máy tính cá nhân; máy chủ và các thiết bị mạng.

2. Thuật ngữ và định nghĩa

- Website: Trang/cổng thông tin điện tử của Sở.

- Cán bộ CNTT: Là cán bộ chuyên trách công nghệ thông tin của Sở.

- Lãnh đạo đơn vị: Lãnh đạo Sở hoặc Lãnh đạo các đơn vị trực thuộc Sở.

3. Nội dung quy trình

Sơ đồ quy trình

Người chịu trách nhiệm	Trình tự công việc	Tài liệu liên quan
Lãnh đạo Sở	Yêu cầu kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng	
Lãnh đạo Sở	Phân công cán bộ CNTT thực hiện hoặc lựa chọn đơn vị đủ năng lực để triển khai	
Cán bộ CNTT/ Đơn vị tư vấn, triển khai	Xây dựng kế hoạch kiểm tra, rà soát, đánh giá bảo đảm ATTT mạng	Kế hoạch kiểm tra, rà soát, đánh giá bảo đảm ATTT mạng
Lãnh đạo Sở	Duyệt — Chưa đạt yêu cầu	
Cán bộ CNTT/ Đơn vị tư vấn, triển khai	Thực hiện kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng	

<table>
<tr><td>Cán bộ CNTT/ Đơn vị tư vấn, triển khai</td><td>Phân tích, xác minh
Lập báo cáo nguy cơ, rủi ro, lỗ hổng, mã độc gây mất an toàn thông tin mạng
Xác minh
Loại bỏ các dữ kiện không đúng</td><td>Báo cáo nguy cơ, rủi ro, lỗ hổng, mã độc gây mất ATTT mạng
Hồ sơ báo cáo nguy cơ, rủi ro, lỗ hổng, mã độc gây mất an toàn thông tin mạng</td></tr>
<tr><td>Cán bộ CNTT/ Đơn vị tư vấn, triển khai</td><td>Tổng hợp báo cáo nguy cơ, rủi ro, lỗ hổng, mã độc gây mất an toàn thông tin mạng và đề xuất phương án xử lý, gửi lãnh đạo Sở, thông báo/cảnh bảo đến các đơn vị liên quan và Sở Thông tin và Truyền thông tỉnh.</td><td>Báo cáo kết quả kiểm tra, rà soát, đánh giá bảo đảm ATTT và đề xuất phương án xử lý</td></tr>
<tr><td>Lãnh đạo Sở</td><td>Phân công Cán bộ CNTT/ Đơn vị đủ năng lực để triển khai các phương án xử lý đảm bảo ATTT</td><td>Kế hoạch thực hiện phương án xử lý</td></tr>
<tr><td>Lãnh đạo Sở</td><td>Yêu cầu kiểm tra, rà soát, đánh giá lại sau khi thực hiện phương án xử lý</td><td></td></tr>
<tr><td>Cán bộ CNTT/ Đơn vị tư vấn, triển khai</td><td>Kiểm tra lại
Thực hiện kiểm tra, rà soát lại nguy cơ, rủi ro, lỗ hổng, mã độc sau khi đã thực hiện phương án xử lý
Báo cáo lãnh đạo đơn vị và Sở Thông tin và Truyền thông tỉnh</td><td>Báo cáo nguy cơ, rủi ro, lỗ hổng, mã độc sau khi đã thực hiện phương án xử lý</td></tr>
<tr><td>Cán bộ CNTT/ Đơn vị tư vấn, triển khai</td><td>Lưu hồ sơ</td><td></td></tr>
</table>

4. Mô tả quy trình

Bước 1: Yêu cầu kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin

Căn cứ vào nhu cầu thực tế và tình hình an ninh, an toàn thông tin trong khu vực hoặc đề nghị hỗ trợ từ các đơn vị trực thuộc Sở. Lãnh đạo Sở xác định yêu cầu kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng (bao gồm: đối tượng, phạm vi kiểm tra, rà soát, đánh giá an toàn bảo mật).

Bước 2: Phân công cán bộ CNTT của Sở thực hiện hoặc lựa chọn đơn vị đủ năng lực để triển khai.

Lãnh đạo cơ quan, đơn vị xem xét năng lực kỹ thuật của cán bộ CNTT để

phân công thực hiện hoặc có thể thuê đơn vị tư vấn phối hợp kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin.

Bước 3: Xây dựng kế hoạch kiểm tra, rà soát, đánh giá bảo đảm ATTT mạng

Cán bộ CNTT hoặc đơn vị tư vấn, triển khai chịu trách nhiệm lập Kế hoạch kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin theo yêu cầu của cơ quan, đơn vị. Kế hoạch kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng phải bao gồm tối thiểu các nội dung sau:

- Mục đích kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng;

- Đối tượng kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin;

- Phạm vi, quy mô kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng;

- Tiêu chí, phương thức kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng;

- Thời gian, kế hoạch thực hiện kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng.

Bước 4. Duyệt kế hoạch kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng

Lãnh đạo Sở xem xét và phê duyệt kế hoạch kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng để Cán bộ CNTT hoặc đơn vị tư vấn tiến hành triển khai thực hiện.

Bước 5. Thực hiện kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin

Cán bộ CNTT hoặc đơn vị tư vấn, triển khai tiến hành kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng các đối tượng:

- Kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng cho trang thông tin điện tử (Website);

- Kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng cho hệ thống ứng dụng công nghệ thông tin;

- Kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng cho máy tính cá nhân;

- Kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng cho máy chủ;

- Kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng cho thiết bị mạng.

- Kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng cho các hệ

thống thông tin khác.

Bước 6. Phân tích xác minh

Cán bộ CNTT hoặc đơn vị tư vấn, triển khai lập báo cáo nguy cơ, rủi ro, lỗ hổng, mã độc gây mất an toàn thông tin mạng. Sau đó phân tích, xem xét báo cáo nguy cơ, rủi ro, lỗ hổng, mã độc gây mất an toàn thông tin mạng để xác nhận lại có đúng nguy cơ mất an toàn thông tin không. Nếu không đúng tiến hành loại bỏ các dữ liệu sự kiện không chính xác. Nếu đúng tiến hành tổng hợp báo cáo nguy cơ, lỗ hổng, mã độc gây mất an toàn thông tin mạng và đề xuất phương án xử lý.

Bước 7. Tổng hợp báo cáo nguy cơ, lỗ hổng, mã độc gây mất an toàn thông tin mạng và đề xuất phương án xử lý

Cán bộ CNTT hoặc đơn vị tư vấn, triển khai tổng hợp kết quả dựa trên kế hoạch kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng, tổng hợp báo cáo nguy cơ, lỗ hổng, mã độc gây mất an toàn thông tin mạng và đề xuất phương án xử lý, gửi Lãnh đạo Sở, đồng thời thông báo/cảnh báo đến các đơn vị liên quan và báo cáo Sở Thông tin và Truyền thông tỉnh.

Bước 8. Phân công Cán bộ CNTT thực hiện hoặc lựa chọn đơn vị đủ năng lực để triển khai các phương án xử lý đảm bảo an toàn thông tin mạng

Cơ quan, đơn vị sau khi nhận báo cáo sẽ xem xét kết quả kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng, nếu còn có những vấn đề vướng mắc thì liên hệ với Cán bộ CNTT hoặc đơn vị tư vấn, triển khai để làm rõ kết quả. Nếu không vướng mắc thì tiến hành các phương án xử lý bảo an toàn thông tin cho hệ thống.

Bước 9. Yêu cầu kiểm tra, rà soát, đánh giá lại sau thực hiện phương án xử lý

Lãnh đạo Sở yêu cầu Cán bộ CNTT hoặc đơn vị tư vấn triển khai tiến hành kiểm tra, rà soát, đánh giá lại các nguy cơ mất an toàn thông tin sau khi thực hiện phương án xử lý.

Bước 10. Kiểm tra lại

Cán bộ CNTT hoặc đơn vị tư vấn thực hiện kiểm tra, rà soát lại nguy cơ, lỗ hổng, mã độc đã thực hiện phương án xử lý để đảm bảo an toàn bảo mật các đối tượng được kiểm tra, rà soát đánh giá như kế hoạch.

Sau khi rà soát tiến hành báo cáo cho Lãnh đạo Sở, các đơn vị liên quan và Sở Thông tin và Truyền thông về kết quả kiểm tra, rà soát, đánh giá.

Bước 11. Lưu hồ sơ

Toàn bộ các hồ sơ trong quá trình kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng được lưu trữ phục vụ các hoạt động quản lý và theo dõi định kỳ.

5. Hồ sơ lưu trữ

STT	Tên hồ sơ	Đơn vị lưu trữ
1.	Kế hoạch kiểm tra, rà soát, đánh giá bảo đảm an toàn thông tin mạng	Văn phòng Sở/Đơn vị tư vấn, triển khai
2.	Báo cáo nguy cơ, lỗ hổng, mã độc gây mất an toàn thông tin mạng	
3.	Hồ sơ báo cáo nguy cơ, lỗ hổng, mã độc gây mất an toàn thông tin mạng	
4.	Báo cáo kết quả kiểm tra, rà soát, đánh giá bảo đảm ATTT và để xuất phương án xử lý	
5.	Báo cáo nguy cơ, lỗ hổng, mã độc sau khi đã thực hiện phương án xử lý	

Phụ lục 02

QUY TRÌNH XỬ LÝ SỰ CỐ AN TOÀN THÔNG TIN MẠNG

(Kèm theo Công văn số 735/SNN-VP, ngày 08/5/2019
của Sở Nông nghiệp và PTNT)

1. Mục đích

Tài liệu này hướng dẫn các bước thực hiện xử lý sự cố an toàn thông tin tại Sở hoặc các đơn vị trực thuộc khi có phát sinh.

2. Phạm vi áp dụng: Sở Nông nghiệp và Phát triển nông thôn

3. Thuật ngữ và định nghĩa

- **Phishing**: Là hành vi giả mạo như là một thực thế đáng tin cậy (website của các cơ quan, tổ chức, các website xã hội phổ biến, các trung tâm chi trả trực tuyến, ...) để lấy cấp thông tin nhạy cảm như tên người dùng, mật khẩu, các chi tiết thẻ tín dụng... thông qua các giao tiếp trên mạng.

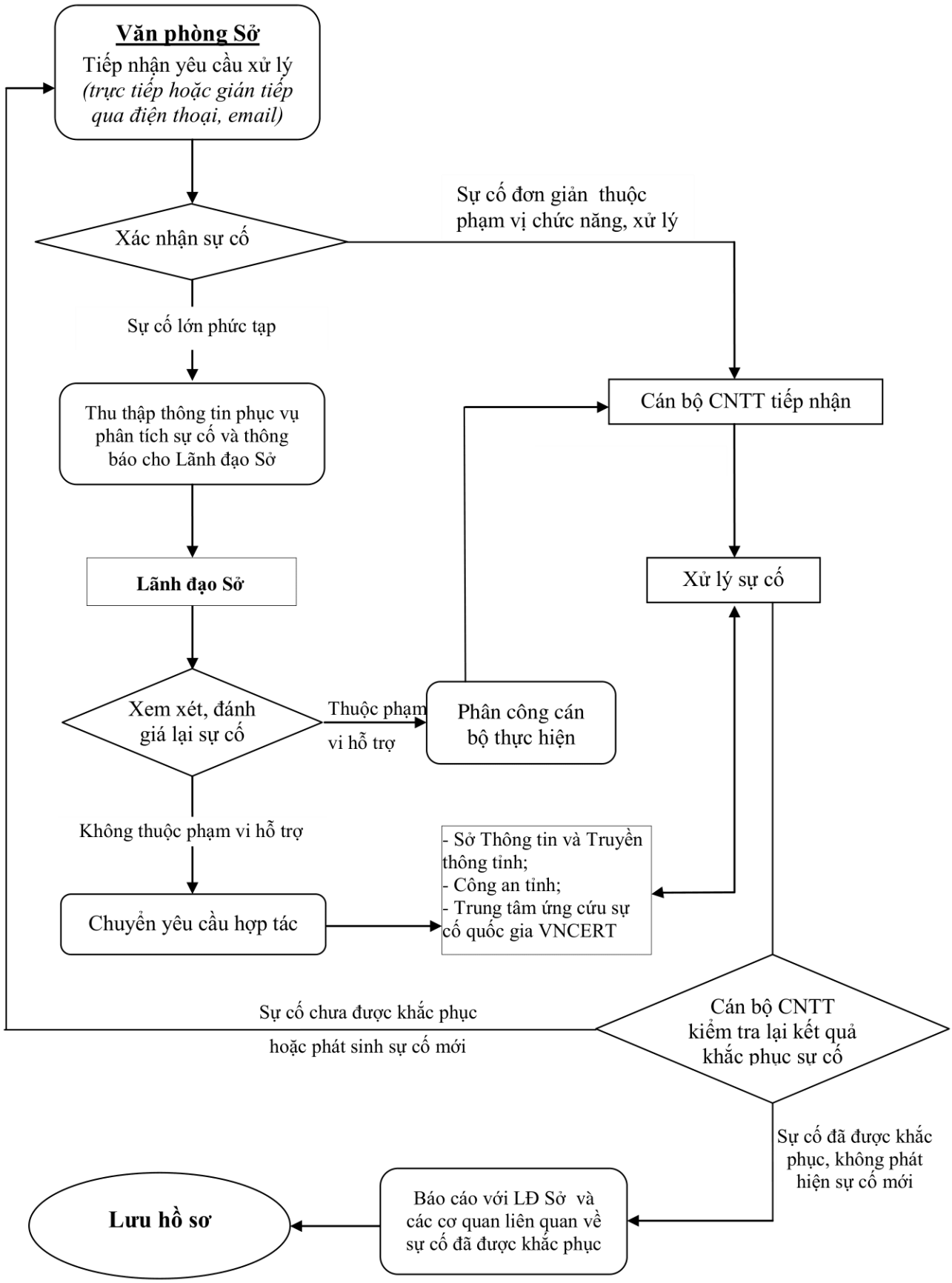
- **Deface**: Là tấn công thay đổi nội dung website của nạn nhân thông qua lỗ hổng bảo mật.

- **Phát tán Malware**: là hành vi phát tán các phần mềm độc hại (virus, trojan, backdoor...) qua môi trường internet.

- **DoS** (Denial of Service) - tấn công từ chối dịch vụ bằng cách chiếm dụng một lượng lớn tải nguyên mạng, tài nguyên hệ thống như băng thông, bộ nhớ, khả năng xử lý ... và làm mất khả năng đáp ứng yêu cầu dịch vụ từ các khách hàng khác.

4. Nội dung quy trình

4.1. Sơ đồ quy trình


Văn phòng Sở
Tiếp nhận yêu cầu xử lý
(trực tiếp hoặc gián tiếp qua điện thoại, email)
Xác nhận sự cố
Sự cố đơn giản thuộc phạm vi chức năng, xử lý
Sự cố lớn phức tạp
Thu thập thông tin phục vụ phân tích sự cố và thông báo cho Lãnh đạo Sở
Cán bộ CNTT tiếp nhận
Lãnh đạo Sở
Xử lý sự cố
Xem xét, đánh giá lại sự cố
Thuộc phạm vi hỗ trợ
Phân công cán bộ thực hiện
Không thuộc phạm vi hỗ trợ
- Sở Thông tin và Truyền thông tỉnh;
- Công an tỉnh;
- Trung tâm ứng cứu sự cố quốc gia VNCERT
Chuyển yêu cầu hợp tác
Sự cố chưa được khắc phục hoặc phát sinh sự cố mới
Cán bộ CNTT kiểm tra lại kết quả khắc phục sự cố
Sự cố đã được khắc phục, không phát hiện sự cố mới
Báo cáo với LĐ Sở và các cơ quan liên quan về sự cố đã được khắc phục
Lưu hồ sơ

4.2. Mô tả quy trình

Bước 1: Tiếp nhận sự cố

Cán bộ CNTT Văn phòng Sở tiếp nhận thông tin về sự cố qua các phương thức: Email, điện thoại, công văn hoặc thông báo sự cố từ các hệ thống giám sát của các cơ quan nhà nước có thẩm quyền như VNCERT, Công an tỉnh hoặc Sở Thông tin và Truyền thông tỉnh.

Bước 2. Xác nhận sự cố và phân loại sự cố

- Xác nhận sự cố: Cán bộ CNTT Văn phòng Sở xác nhận sự cố bao gồm các thông tin như sau:

+ Tình trạng (Sự cố sẽ xảy ra; Sự cố đang xảy ra; Sự cố đã xảy ra);

+ Mức độ (Sự cố nghiêm trọng; Sự cố bình thường);

+ Phạm vi (Sự cố diện rộng; Sự cố mạng máy tính; Sự cố một máy tính);

+ Và địa điểm xảy ra sự cố.

- Phân loại sự cố: Sau khi xác nhận được sự cố, Cán bộ CNTT có trách nhiệm phân loại các sự cố.

Trường hợp:

+ Sự cố đơn giản thuộc phạm vi hỗ trợ, cán bộ CNTT sẽ trực tiếp hỗ trợ, xử lý.

+ Sự cố lớn phức tạp báo cáo Lãnh đạo Sở xem xét, chuyển yêu cầu hỗ trợ đến các cơ quan chức năng.

Bước 3. Báo cáo Lãnh đạo Sở, xin ý kiến chỉ đạo

Ngay sau khi phân loại được sự cố cán bộ CNTT có trách nhiệm báo cáo Lãnh đạo Sở để xem xét loại sự cố và tuỳ theo đối tượng sẽ tiến hành phân công cán bộ CNTT ứng cứu sự cố và thông báo với các đơn vị có liên quan để được hỗ ứng cứu sự cố.

Trường hợp phức tạp không tự xử lý được, gửi công văn nhờ sự hỗ trợ của nhà cung cấp dịch vụ Internet và các cơ quan chuyên trách như Sở Thông tin và Truyền thông tỉnh, Công an tỉnh hoặc Trung tâm ứng cứu sự cố quốc gia VNCERT.

Bước 4. Thu thập thông tin phục vụ phân tích sự cố

Sau khi nhận được công văn đề nghị hỗ trợ của Sở. Cơ quan chuyên trách ứng cứu sự cố sẽ cử cán bộ phối hợp với Cán bộ CNTT tiến hành thu thập các thông tin:

- Thông tin về đầu mối liên hệ.

- Thu thập thông tin hệ thống.

- Thu thập trạng thái network và các kết nối.

- Thu thập các tiến trình đang chạy.

- Thu thập ổ cứng.

- Thu thập Log file.

Bước 5. Phân tích sự cố

Cán bộ CNTT của Sở phối hợp cùng đơn vị hỗ trợ tiến hành phân tích sự cố, bao gồm các thông tin sau:

- Phân tích dòng thời gian

- Thời gian bị sửa đổi, truy cập, tạo hoặc thay đổi

- Thời gian thực hiện các cập nhật lớn đối với hệ thống

- Thời điểm mà hệ thống sử dụng lần cuối cùng

- Phân tích dữ liệu

- Kiểm tra sự thay đổi cấu hình

- Kiểm tra hệ thống tập tin có bị mã độc

- Kiểm tra tập tin Internet history và các tập tin history khác

- Kiểm tra Registry và tiến trình

- Quan sát các tập tin, tiến trình lúc khởi động

- Phân tích log file

Bước 6. Xử lý sự cố

Cán bộ CNTT của Sở phối hợp cùng đơn vị hỗ trợ tiến hành xử lý sự cố bao gồm các công việc sau:

- Gỡ bỏ sự cố

- Xác định và loại bỏ các backdoors, phishing, Deface, Malware, DoS…..

- Phân tích và kiểm tra lỗ hổng sau khi thực hiện các bản vá lỗi

- Khôi phục dữ liệu

- Thu thập các tập tin, hình ảnh, email,... bị xóa, thời gian bị xóa

- Tìm kiếm các tập tin không thể khôi phục

- Khôi phục các tập tin phù hợp

Bước 7. Tổng hợp báo cáo

Cán bộ CNTT của Sở phối hợp cùng đơn vị hỗ trợ tiến hành tổng hợp kết quả phân tích và báo cáo kết quả với Lãnh đạo Sở và các cơ quan chuyên trách như Sở Thông tin và Truyền thông tỉnh, Công an tỉnh hoặc Trung tâm ứng cứu sự cố quốc gia VNCERT. Trong đó mô tả chi tiết các bước thực hiện, giải pháp xử lý sự cố, kết quả khắc phục hiện tại và đề xuất các biện pháp ứng dụng cho các sự cố tương tự.

Bước 8. Lưu hồ sơ

Toàn bộ các hồ sơ trong quá trình xử lý sự cố được lưu trữ phục vụ các hoạt động quản lý và theo dõi định kỳ.

STT	Tên hồ sơ	Đơn vị lưu trữ
1.	Thông báo sự cố	Văn phòng Sở
2.	Kế hoạch xử lý sự cố	
3.	Hồ sơ xử lý sự cố	
4.	Báo cáo phân tích kết quả điều tra xử lý sự cố	
5.	Báo cáo thông kê hàng năm	