UỶ BAN NHÂN DÂN TỈNH THANH HOÁ **SỞ NÔNG NGHIỆP VÀ PTNT**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 88 /KH-SNN&PTNT	*Thanh Hoá, ngày 25 tháng 11 năm 2022*

KẾ HOẠCH
Bảo đảm an toàn thông tin mạng và triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng

Thực hiện Chỉ thị số 13/CT-UBND ngày 04/11/2022 của UBND tỉnh về việc đẩy mạnh bảo đảm an toàn thông tin mạng và triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng. Sở Nông nghiệp và PTNT xây dựng Kế hoạch bảo đảm an toàn thông tin mạng và triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng, cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích:

- Đảm bảo an toàn thông tin cho các hệ thống thông tin của Sở Nông nghiệp và PTNT; đảm bảo khả năng thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa mất an toàn thông tin trên mạng; đề ra các giải pháp ứng phó sự cố mất an toàn thông tin mạng.

- Tạo chuyển biến mạnh mẽ trong nhận thức về an toàn thông tin đối với cán bộ, công chức, viên chức, người lao động thuộc Sở.

- Đảm bảo các nguồn lực và các điều kiện cần thiết để sẵn sàng triển khai kịp thời, hiệu quả các phương án ứng cứu khẩn cấp sự cố an toàn thông tin mạng.

2. Yêu cầu:

- Triển khai và thực hiện tốt công tác bảo đảm ATTT mạng theo chỉ đạo tại Chỉ thị số 41-CT/TW ngày 24/3/2020 của Ban Bí thư Trung ương Đảng về tăng cường phối hợp và triển khai đồng bộ các biện pháp bảo đảm an toàn, an ninh mạng; Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam; Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố ATTT mạng Việt Nam và các văn bản chỉ đạo, hướng dẫn của Bộ Thông tin và Truyền thông, của Chủ tịch UBND tỉnh liên quan đến công tác ATTT mạng và ứng cứu sự cố ATTT mạng.

II. NỘI DUNG TRIỂN KHAI

1. Nguyên tắc triển khai

- Tổ chức phổ biến, quán triệt tới các đơn vị cơ sở, cán bộ, công chức, viên chức, người lao động các nguyên tắc:

+ Ứng cứu sự cố ATTT mạng là hoạt động quan trọng nhằm phát hiện, ngăn chặn, xử lý và khắc phục kịp thời sự cố ATTT mạng.

+ Hệ thống thông tin được kiểm tra, đánh giá ATTT mạng trước khi đưa vào sử dụng.

- Thủ trưởng các cơ quan, đơn vị trực tiếp chịu trách nhiệm trước Giám đốc Sở nếu để xảy ra sự cố mất ATTT mạng, để xảy ra hậu quả, thiệt hại nghiêm trọng tại cơ quan, đơn vị thuộc phạm vi quản lý.

2. Đảm bảo an toàn hệ thống thông tin

- Tổ chức triển khai bảo đảm ATTT mạng đầy đủ theo mô hình 4 lớp tại các cơ quan, đơn vị, bao gồm:

+ Lực lượng tại chỗ.

+ Tổ chức hoặc doanh nghiệp giám sát, bảo vệ chuyên nghiệp.

+ Tổ chức hoặc doanh nghiệp độc lập kiểm tra, đánh giá định kỳ.

+ Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia.

- Xây dựng Hồ sơ đề xuất cấp độ và trình các cấp có thẩm quyền thẩm định và phê duyệt cấp độ an toàn hệ thống thông tin; hoàn thành trước ngày 01/12/2022. Bảo đảm các hệ thống thông tin được triển khai đầy đủ phương án bảo đảm an toàn hệ thống thông tin theo cấp độ trước ngày 01/6/2023.

3. Phương thức hoạt động

- Hoạt động ứng cứu sự cố ATTT mạng phải chuyển từ bị động sang chủ động, bao gồm: Chủ động thực hiện săn lùng mối nguy hại và rà quét lỗ hổng trên các hệ thống thông tin trong phạm vi quản lý tối thiểu 01 lần/6 tháng.

- Rà soát, ban hành phương án, kịch bản ứng cứu sự cố cho hệ thống thông tin trước ngày 31/12/2022 và cập nhật kịp thời khi có thay đổi.

- Tổ chức diễn tập thực chiến tối thiểu 01 lần/năm đối với hệ thống thông tin cấp độ 3 trở lên nhằm đánh giá khả năng phòng ngừa xâm nhập và khả năng phát hiện kịp thời các điểm yếu về quy trình, công nghệ, con người. Trường hợp phát hiện điểm yếu, lỗ hổng bảo mật cho phép xâm nhập và kiểm soát hệ thống thì thực hiện đồng thời khắc phục điểm yếu, lỗ hổng và săn lùng mối nguy hại.

4. Kiện toàn tổ chức

Tổ chức, kiện toàn lại Tổ ứng cứu sự cố ATTT mạng của Sở Nông nghiệp và PTNT theo hướng chuyên nghiệp, cơ động, khuyến khích có sự tham gia của chuyên gia ATTT mạng đáp ứng chuẩn kỹ năng về ATTT do Bộ Thông tin và Truyền thông quy định.

Đối với Hệ thống thông tin của các đơn vị trực thuộc: Chủ động thực hiện giám sát, ứng cứu sự cố an toàn thông tin mạng, bảo vệ hệ thống thông tin thuộc quyền quản lý hoặc lựa chọn tổ chức, doanh nghiệp có đủ năng lực để thực hiện; thường xuyên rà soát, cử cán bộ đầu mối (phụ trách/kiêm nhiệm) chịu trách nhiệm về ATTT

mạng tại cơ quan, đơn vị, phối hợp chặt chẽ với Tổ ứng cứu sự cố ATTT mạng của Sở, Sở Thông tin và Truyền thông, Đội ứng cứu sự cố ATTT mạng của tỉnh trong công tác đảm bảo ATTT mạng cho các hệ thống thông tin trên địa bàn tỉnh.

5. Bảo vệ bí mật nhà nước

Không lưu trữ cơ sở dữ liệu, tài liệu có chứa thông tin thuộc phạm vi bí mật nhà nước trên máy tính có kết nối mạng Internet, mạng nội bộ. Kiểm tra an toàn, an ninh thông tin đối với các thiết bị điện tử, giải pháp công nghệ trước khi đưa vào sử dụng tại các bộ phận trọng yếu, cơ mật; loại bỏ triệt để thông tin, tài liệu khi chuyển đổi mục đích sử dụng các thiết bị đã lưu dữ liệu, tài liệu có chứa thông tin thuộc phạm vi bí mật nhà nước. Kiểm soát việc sửa chữa, thay thế trang thiết bị máy tính trong cơ quan, đơn vị nhằm hạn chế việc lộ, mất thông tin, dữ liệu.

6. Đảm bảo an toàn thông tin mạng

- Chỉ kết nối đến các hệ thống thông tin, ứng dụng dùng chung của tỉnh tại các cơ quan, đơn vị thông qua mạng Truyền số liệu chuyên dùng của tỉnh. Đối với các phần mềm dùng chung, phần mềm chuyên ngành cán bộ, công chức, viên chức, người lao động được cấp tài khoản riêng, yêu cầu thường xuyên thay đổi mật khẩu truy cập. Khi trao đổi thông tin phục vụ công việc nhà nước, yêu cầu sử dụng hệ thống thư điện tử công vụ dùng chung của tỉnh, của ngành, không sử dụng thư điện tử thương mại, thư điện tử công cộng.

- Thường xuyên rà soát, thực hiện nâng cấp, chuẩn hóa hạ tầng kỹ thuật công nghệ thông tin, an toàn, an ninh mạng. Nghiêm túc thực hiện khắc phục kịp thời các lỗ hổng, điểm yếu theo cảnh báo của cơ quan chức năng; chủ động theo dõi, phát hiện sớm các nguy cơ mất ATTT mạng để kịp thời xử lý, khắc phục. Có biện pháp kiểm soát nguy cơ mất ATTT mạng gây ra bởi bên thứ ba và các chuỗi cung ứng công nghệ thông tin và truyền thông.

- Nghiêm túc thực hiện các quy định về báo cáo sự cố ATTT mạng; đẩy mạnh tuyên truyền cho người dân về việc báo cáo, cung cấp thông tin sự cố. Khuyến khích triển khai các chiến dịch nâng cao ý thức cảnh giác của người dùng cuối đối với các cuộc tấn công mạng.

III . KINH PHÍ THỰC HIỆN

- Kinh phí thực hiện kế hoạch được bố trí từ nguồn ngân sách nhà nước, nguồn xã hội hóa và các nguồn vốn huy động hợp pháp khác.

- Căn cứ Thông tư số 121/2018/TT-BTC ngày 12/12/2018 của Bộ trưởng Bộ Tài chính quy định về lập dự toán, quản lý, sử dụng và quyết toán kinh phí thực hiện công tác ứng cứu sự cố, đảm bảo an toàn thông tin.

VI. TỔ CHỨC THỰC HIỆN

- Văn phòng Sở tổ chức công tác kiểm tra, giám sát, hướng dẫn, hỗ trợ các đơn vị trực thuộc trong việc thực hiện các nhiệm vụ của Kế hoạch.

- Các phòng, đơn vị trực thuộc Sở tổ chức thực hiện Kế hoạch này, đảm bảo

thực hiện nhiệm vụ an toàn thông tin mạng trong phạm vi quản lý phù hợp với điều kiện thực tế; trước ngày 05/12 hàng năm (hoặc đột xuất) báo cáo Sở Nông nghiệp và PTNT kết quả thực hiện; rà soát, đổi mật khẩu đăng nhập TDOffice cho toàn bộ cán bộ, công chức, viên chức trước ngày **05/12/2022** *(áp dụng cho các tài khoản đang để mật khẩu mặc định)*.

Trên đây là Kế hoạch Bảo đảm an toàn thông tin mạng và triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng của Sở Nông nghiệp và PTNT. Trong quá trình thực hiện nếu có khó khăn, vướng mắc, các cơ quan, đơn vị phản ánh kịp thời về Văn phòng Sở để phối hợp giải quyết./.

Nơi nhận:
- Sở Thông tin và Truyền thông (tổng hợp);
- Lãnh đạo Sở (báo cáo);
- Các Phòng Sở (để t/h);
- Các đơn vị trực thuộc (để t/h);
- Lưu: VT, VP.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Lê Đức Thuận