

Số: /BC-SKHCN

Hưng Yên, ngày tháng năm 2024

BÁO CÁO

Kết quả thực hiện phương án đảm bảo an toàn thông tin của Sở Khoa học và Công nghệ

Ngày 18/3/2024 Sở Khoa học và Công nghệ nhận được Công văn số 333/STTTT-BCVTCNTT về việc xây dựng hồ sơ đề xuất cấp độ an toàn thông tin và triển khai đầy đủ phương án đảm bảo an toàn thông tin (ATTT) theo nghị định 85/2016/NĐ-CP, Sở Khoa học và Công nghệ báo cáo như sau:

I. ĐÁNH GIÁ KẾT QUẢ THỰC HIỆN

Sở Khoa học và Công nghệ đã xây dựng và được Sở Thông tin và Truyền thông phê duyệt cấp độ an toàn ở cấp độ 2 cho 03 hệ thống thông tin, gồm: Hệ thống Sàn giao dịch công nghệ tỉnh Hưng Yên; Hệ thống Cổng thông tin điện tử Sở Khoa học và Công nghệ; Hệ thống Trang thông tin điện tử Chi cục Tiêu chuẩn Đo lường chất lượng tỉnh Hưng Yên. Các hệ thống trên sử dụng hạ tầng dùng chung của Trung tâm tích hợp dữ liệu của tỉnh.

1. Thiết lập chính sách an toàn thông tin

1.1. Chính sách an toàn thông tin

- Các hệ thống thông tin của Sở đã đáp ứng Chính sách an toàn thông tin.
- Đáp ứng các yêu cầu về Quản lý an toàn máy chủ và ứng dụng.
- Đáp ứng các yêu cầu về Quản lý an toàn dữ liệu.
- Các thiết bị đầu cuối khi kết nối vào các hệ thống đã được quản lý.

1.2. Xây dựng và công bố

Sở Khoa học và Công nghệ tiến hành xây dựng dự thảo Quy chế bảo đảm an toàn thông tin cho Cổng Thông tin điện tử Sở theo Nghị định số 85/2016/NĐ-CP ngày 01 tháng 07 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ. Quy chế được lấy ý kiến các phòng, đơn vị trực thuộc Sở trước khi hoàn thiện ban hành áp dụng.

1.3. Rà soát, sửa đổi

Tiến hành rà soát, sửa đổi Quy chế bảo đảm an toàn thông tin: Định kỳ 03 năm hoặc khi có thay đổi Quy chế bảo đảm an toàn thông tin, kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.

2. Tổ chức bảo đảm an toàn thông tin

2.1. Đơn vị chuyên trách về an toàn thông tin

Sở Khoa học và Công nghệ giao Trung tâm Thông tin, Thống kê, Ứng dụng KH&CN, Chi cục Tiêu chuẩn Đo lường Chất lượng trực tiếp quản lý, vận hành và chịu trách nhiệm về an toàn thông tin của 03 hệ thống thông tin của Sở.

2.2. Phối hợp với những cơ quan/tổ chức có thẩm quyền

Sở Khoa học và Công nghệ giao Phòng Công nghệ và Đổi mới sáng tạo chịu trách nhiệm đầu mối về quản lý công nghệ thông tin của Sở. Chủ trì, phối hợp với các đơn vị trong xây dựng và thực hiện an toàn thông tin mạng. Chịu trách nhiệm quản lý, báo cáo về lĩnh vực quản lý thông tin, thống kê và công nghệ thông tin đảm bảo an toàn mạng trước Giám đốc Sở, thường xuyên nắm bắt và báo cáo kịp thời về khả năng phát triển thông tin, phát triển các hệ thống thông tin của Sở về đảm bảo an toàn thông tin mạng.

Phối hợp với Sở Thông tin và Truyền thông thực hiện các phương án đảm bảo an toàn, an ninh thông tin.

3. Bảo đảm nguồn nhân lực

Hiện nay, Sở Khoa học và Công nghệ có 01 công chức kiêm nhiệm quản lý hoạt động công nghệ thông tin của Sở. Chi cục Tiêu chuẩn Đo lường Chất lượng; Trung tâm Thông tin, Thống kê và Ứng dụng KH&CN có công chức, viên chức chuyên môn về công nghệ thông tin.

4. Quản lý thiết kế, xây dựng hệ thống

Có quy định về thiết kế an toàn hệ thống thông tin.

Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.

Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ.

Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.

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. Quản lý vận hành hệ thống

5.1. Quản lý an toàn mạng

Xây dựng quy chế, quy trình vận hành 03 hệ thống thông tin của Sở. Đến nay các hệ thống thông tin Sở đang được vận hành tốt. Các hệ thống được cập nhật; sao lưu dự phòng các tập tin cấu hình hệ thống và khôi phục hệ thống sau khi xảy ra sự cố. Giao quyền truy cập và quản lý cấu hình hệ thống trực tiếp cho công chức, viên chức để đảm bảo an toàn và phối hợp quản lý, vận hành tốt các hệ thống thông tin theo quy định.

5.2. Quản lý an toàn máy chủ và ứng dụng

Sở Khoa học và Công nghệ giao các đơn vị trực thuộc quản lý, vận hành các hệ thống thông tin. Cập nhật, sao lưu dự phòng các tập tin cấu hình hệ thống và khôi phục hệ thống sau khi xảy ra sự cố. Thường xuyên, định kỳ sử dụng giải

pháp chuyên dụng hoặc giải pháp tương đương sử dụng các giải pháp như SAN, NAS... để tiến hành cập nhật hệ thống, phần mềm, đề đồng bộ hóa hệ thống. Tiến hành sao lưu dự phòng thường xuyên dữ liệu nhằm khôi phục dữ liệu và khắc phục khi có sự cố xảy ra.

5.3. Quản lý an toàn dữ liệu

Sở có quy định dự phòng và khôi phục dữ liệu thường xuyên, định kỳ 01 tháng sao lưu các dữ liệu hệ thống và tự sao lưu dữ liệu cập nhật trong 24 giờ.

Xây dựng quy trình thực hiện các bước sao lưu dữ liệu và khôi phục dữ liệu khi sự cố xảy ra. Dữ liệu sao lưu dự phòng được lưu trữ trên máy tính khác của Trung tâm. Đảm bảo các quy định về an toàn dữ liệu.

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.

5.4. Quản lý an toàn thiết bị đầu cuối

Xây dựng phương án phân nhóm sự cố an toàn thông tin mạng như: hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ để có giải pháp phòng chống các mã độc xâm hại. Khi phát hiện các mã độc xâm hại có thể nhanh chóng khoanh vùng và xử lý loại bỏ mã nguồn độc và khắc phục khôi phục dữ liệu hoặc sử dụng dữ liệu dự phòng để khôi phục.

Xây dựng, ban hành văn bản chỉ đạo điều hành, văn bản hướng dẫn về công tác giám sát, đảm bảo an toàn thông tin mạng trong hoạt động của toàn Sở; Ban hành kế hoạch triển khai nhiệm vụ giám sát, ứng phó sự cố an toàn thông tin mạng hàng năm lồng ghép vào nội dung Kế hoạch ứng dụng CNTT của Sở KH&CN...

Xây dựng, duy trì hệ thống giám sát, đảm bảo an toàn thông tin của Sở: Thành lập tổ giám sát, kiểm soát an toàn thông tin, giao Trung tâm Thông tin, Thống kê và Ứng dụng KH&CN làm thường trực; Thực hiện quan trắc, giám sát an toàn thông tin mạng cho các hệ thống dùng chung của Sở; Triển khai kiểm tra, rà soát, đánh giá an toàn, an ninh thông tin mạng; Triển khai giám sát an toàn thông tin mạng cho phần dịch vụ, hạ tầng mạng phục vụ xây dựng Chính quyền điện tử của toàn Sở.

Thường xuyên đề xuất, cử cán bộ đi đào tạo, tập huấn và tuyên truyền về an toàn thông tin.

5.5. Quản lý an toàn người sử dụng đầu cuối.

Sở đã ban hành quy chế quản lý mạng và sử lý mạng máy tính nội bộ trên cơ sở sau: Cấp quyền truy cập cho Lãnh đạo Sở, admin và quyền truy cập thông thường cho các công chức, viên chức và người lao động.

Công chức, viên chức và người lao động được quyền truy cập để sử dụng nguồn tài nguyên dữ liệu nội bộ, các file được chuyển tải phục vụ công tác quản

lý, chuyên môn,...thông qua tài khoản được cấp và mật khẩu đăng nhập, phải thường xuyên thay đổi mật khẩu đăng nhập để đảm bảo an toàn và bảo mật dữ liệu trên mạng nội bộ.

Người dùng có thể truyền file, đăng tải các thông tin và được admin kiểm duyệt trước khi đăng. Việc truy cập và sử dụng tài nguyên nội bộ phải tuân thủ theo quy định và phải đảm bảo an ninh, bảo mật mạng nội bộ.

II. KIẾN NGHỊ, ĐỀ XUẤT

Đề nghị Ủy ban nhân dân tỉnh quan tâm, giao biên chế đặc thù theo vị trí việc làm về công nghệ thông tin, nhằm đảm bảo nguồn nhân lực cho chuyển đổi số và tham mưu vận hành các hệ thống, nền tảng công nghệ thông tin đáp ứng yêu cầu chuyển đổi số của các cấp, các ngành. Tổ chức các khóa đào tạo, tập huấn về công nghệ thông tin, chuyển đổi số.

Sở Khoa học và Công nghệ gửi Sở Thông tin và Truyền thông tổng hợp./.

**KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Nơi nhận:

- Sở Thông tin và Truyền thông;
- Giám đốc và các PGĐ Sở;
- Các phòng, đơn vị trực thuộc Sở;
- Lưu: VT, CNĐMST.

Nguyễn Xuân Hải