

Số: /QĐ-CNTY

Lào Cai, ngày tháng 4 năm 2024

QUYẾT ĐỊNH

Ban hành Nội quy đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Chi cục Chăn nuôi và Thú y tỉnh Lào Cai

CHI CỤC TRƯỞNG CHI CỤC CHĂN NUÔI VÀ THÚ Y TỈNH LÀO CAI

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

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

Căn Luật An ninh mạng ngày 12 tháng 6 năm 2016;

Căn cứ các văn bản hướng dẫn thi hành Luật Công nghệ thông tin năm 2006, Luật An toàn thông tin mạng năm 2015, Luật An ninh mạng năm 2016 và các văn bản liên quan;

Căn cứ Quyết định số 61/2021/QĐ-UBND ngày 31/12/2021 của UBND tỉnh Lào Cai về ban hành Quy chế đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin trong các cơ quan nhà nước trên địa bàn tỉnh Lào Cai;

Căn cứ Quyết định số 27/2022/QĐ-UBND ngày 28/7/2022 của UBND tỉnh Lào Cai Ban hành Quy định vị trí, chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Chi cục Chăn nuôi và Thú y tỉnh Lào Cai;

Căn cứ Kế hoạch số 93/KH-SNN ngày 31/08/2023 của Sở Nông nghiệp và PTNT về việc triển khai thực hiện chiến lược an toàn, an ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn đến năm 2030;

Căn cứ Văn bản số 573/SNN-VP ngày 27/3/2024 của Sở Nông nghiệp và PTNT về việc chấn chỉnh công tác bảo đảm an toàn, an ninh mạng tại các phòng, cơ quan, đơn vị thuộc Sở.

Theo đề nghị của Trưởng phòng Hành chính - Tổng hợp.

QUYẾT ĐỊNH:

Điều 1: Ban hành kèm Quyết định này Nội quy đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Chi cục Chăn nuôi và Thú y tỉnh Lào Cai.

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

Điều 3: Lãnh đạo, công chức, viên chức thuộc Chi cục Chăn nuôi và Thú y tỉnh Lào Cai chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- Sở Nông nghiệp và PTNT (B/c);
- Lãnh đạo Chi cục;
- Trạm Thú y các huyện, thị xã, thành phố;
- Các phòng thuộc Chi cục.
- Lưu: VT, QLDB.

CHI CỤC TRƯỞNG

Phạm Bá Uyên

SỞ NÔNG NGHIỆP VÀ PTNT
TỈNH LÀO CAI
CHI CỤC CHĂN NUÔI VÀ THÚ Y

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

NỘI QUY

Đảm bảo an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Chi cục Chăn nuôi và Thú y tỉnh Lào Cai
(Ban hành kèm theo Quyết định số /QĐ-CNTY ngày tháng 4 năm 2024 của Chi cục Chăn nuôi và Thú y)

Chương I

QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Nội quy này quy định việc bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin (sau đây viết tắt là CNTT) của Chi cục Chăn nuôi và Thú y tỉnh Lào Cai.

Điều 2. Đối tượng áp dụng

Nội quy này áp dụng đối với các phòng, trạm và lãnh đạo, công chức, viên chức, người lao động thuộc Chi cục Chăn nuôi và Thú y tỉnh Lào Cai.

Điều 3. Mục đích, nguyên tắc bảo đảm an toàn thông tin mạng

1. Mục đích:

Việc áp dụng Nội quy này nhằm phòng ngừa, ngăn chặn, xử lý và giảm thiểu các nguy cơ gây mất an toàn thông tin mạng và bảo đảm an toàn thông tin trong quá trình ứng dụng CNTT trong hoạt động của Chi cục.

2. Nguyên tắc:

a) Tổ chức, cá nhân thuộc đối tượng áp dụng Nội quy này có trách nhiệm bảo đảm an toàn thông tin và hệ thống thông tin trong phạm vi xử lý công việc của mình theo quy định của pháp luật, hướng dẫn của cơ quan, đơn vị có thẩm quyền và các quy định tại Nội quy này;

b) Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác;

c) Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức;

d) Hoạt động an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

Điều 4. Các hành vi bị nghiêm cấm

Các hành vi bị nghiêm cấm thực hiện theo quy định tại Điều 7 Luật An toàn thông tin mạng và Điều 8 Luật An ninh mạng.

Chương II

ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG

Điều 5. Quản lý truy cập

1. Quản lý chặt chẽ tài khoản của các hệ thống thông tin. Đối với các phần mềm nghiệp vụ của Chi cục Chăn nuôi và Thú y tỉnh Lào Cai đã cung cấp tài khoản cho công chức, viên chức, người lao động để thực hiện nhiệm vụ thì khi công chức, viên chức, người lao động đã nghỉ việc, chuyển công tác phải hủy tài khoản, quyền truy nhập, thu hồi các thiết bị liên quan tới hệ thống thông tin.

2. Yêu cầu Công chức, viên chức, người lao động khi đặt mật khẩu đăng nhập vào các hệ thống thông tin phải phải đặt mật khẩu có độ an toàn, phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự số và ký tự đặc biệt như !, @, #, \$, %,...) và phải được thay đổi ít nhất 3 tháng/lần.

3. Mỗi công chức, viên chức và người lao động chỉ được phép truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình, có trách nhiệm bảo mật tài khoản truy cập thông tin.

4. Khi sử dụng các ứng dụng dùng chung của tỉnh mọi người phải có ý thức tự bảo vệ thông tin cá nhân của mình; nghiêm cấm việc tiết lộ tài khoản đăng nhập của mình cho người không có thẩm quyền hoặc sử dụng trái phép tài khoản của người khác để truy cập trái phép vào hệ thống các phần mềm dùng chung của tỉnh.

Điều 6. Đảm bảo an toàn, an ninh thông tin

1. Thường xuyên phổ biến, quán triệt và cập nhật những quy định về an toàn thông tin và hướng dẫn công chức, viên chức, người lao động thực hiện đúng hướng dẫn về an toàn, an ninh thông tin nhằm nâng cao nhận thức và trách nhiệm về an toàn thông tin.

2. Bảo vệ bí mật thông tin tài khoản cá nhân hoặc tài khoản của Chi cục khi được phân công nắm giữ, đồng thời phải thay đổi ngay mật khẩu tài khoản khi mới được cấp và tự chịu trách nhiệm trong việc quản lý, bảo vệ mật khẩu của tài khoản, không được cho người khác sử dụng tài khoản cá nhân hoặc của đơn vị.

3. Không đặt chế độ tự động ghi nhớ mật khẩu của các trình duyệt trong mọi trường hợp sử dụng; thường xuyên thay đổi mật khẩu có độ phức tạp cao đối với các tài khoản phục vụ công tác, tài khoản ứng dụng cá nhân.

4. Công chức, viên chức khi được giao trách nhiệm quản lý, sử dụng máy tính phải đặt mật khẩu đăng nhập; đối với máy tính nhiều người sử dụng phải đặt mật khẩu cho tài liệu đảm bảo tính bảo mật công tác.

5. Khi khai thác, sử dụng các phần mềm ứng dụng dùng chung của tỉnh tại các điểm truy cập Internet công cộng, tuyệt đối không đặt chế độ ghi nhớ mật khẩu trong các trình duyệt.

6. Khai thác tài nguyên Internet có chọn lọc, không vào các trang website lạ, không bấm vào các đường liên kết, biểu tượng quảng cáo không rõ nội dung và không cài đặt phần mềm không rõ nguồn gốc.

7. Thường xuyên cập nhật bản vá lỗ hổng bảo mật cho các phiên bản hệ điều hành, phần mềm, ứng dụng theo khuyến cáo của đơn vị phát hành và các chuyên gia về an ninh mạng; cài đặt phần mềm diệt virus bản quyền cho hệ thống máy tính.

8. Không cài đặt các phần mềm ứng dụng không rõ nguồn gốc, chưa được đánh giá tính năng, độ tin cậy...

9. Quản lý, sử dụng các thiết bị lưu trữ thông tin (USB, ổ cứng di động...), điện thoại thông minh đảm bảo an toàn, đúng cách theo quy định tại Chỉ thị số 02/CT-TTg ngày 15/11/2019 của Thủ tướng Chính phủ và Chỉ thị số 02/CT-BCA ngày 17/4/2017 của Bộ Công an.

10. Các thiết bị CNTT dùng để soạn thảo, in ấn văn bản, lưu trữ thông tin bí mật nhà nước của Chi cục phải được bố trí riêng, tiến hành ở nơi đảm bảo bí mật, an toàn; không được kết nối vào mạng LAN của đơn vị. Đặc biệt là không được sử dụng máy tính đã nối mạng Internet đánh máy, in, sao tài liệu mật. Trên máy tính này phải thực hiện các chế độ mã hóa, phân quyền và đặt mật khẩu cho người được giao sử dụng để đảm bảo an toàn, bảo mật thông tin. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các phòng, đơn vị phải báo cáo cho người có thẩm quyền. Không được cho phép các công ty tư nhân hoặc người không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

Điều 7. Phát triển nguồn nhân lực an toàn thông tin

1. Cán bộ kiêm nhiệm về CNTT của Chi cục được tạo điều kiện trang bị các thiết bị tin học, phương tiện kỹ thuật làm việc phù hợp với chuyên môn, yêu cầu công việc; tham dự đầy đủ các khóa đào tạo và bồi dưỡng kiến thức, nghiệp vụ cho cán bộ quản lý, kỹ thuật về an toàn thông tin mạng.

2. Thường xuyên tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức về bảo đảm an toàn, an ninh thông tin mạng đến toàn thể bộ cán bộ, công

chức, viên chức và người lao động của đơn vị.

Chương III

TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 8. Trách nhiệm của Trưởng các phòng, trạm thuộc Chi cục Chăn nuôi và Thú y

1. Tổ chức tuyên truyền, phổ biến quán triệt cho công chức, viên chức và người lao động các văn bản chỉ đạo của Trung ương, của Tỉnh ủy, UBND tỉnh và các quy định của pháp luật về đảm bảo an toàn, an ninh thông tin nhằm nâng cao nhận thức cho công chức, viên chức và người lao động về nguy cơ mất an toàn, an ninh hệ thống thông tin và có biện pháp để phòng ngừa, ngăn chặn khi có sự cố xảy ra.

2. Tổ chức thực hiện các quy định tại Nội quy này và các quy định pháp luật có liên quan; chịu trách nhiệm trước Chi cục trưởng trong công tác đảm bảo an toàn, an ninh thông tin của Chi cục.

3. Khi có sự cố hoặc nguy cơ mất an toàn thông tin phải chỉ đạo xử lý khắc phục kịp thời và thông tin cho phòng Hành chính, tổng hợp. Trường hợp không khắc phục được thì báo phòng Hành chính - tổng hợp đề phòng Hành chính - tổng hợp báo Tổ ứng cứu sự cố máy tính trên địa bàn tỉnh đề hướng dẫn, hỗ trợ khắc phục.

4. Phối hợp chặt chẽ trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động vi 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.

Điều 9. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong các cơ quan, đơn vị

1. Trách nhiệm của cán bộ, công chức phụ trách an toàn thông tin mạng:

a) Chịu trách nhiệm triển khai các biện pháp bảo đảm an toàn thông tin mạng của Chi cục;

b) Tham mưu lãnh đạo Chi cục ban hành các quy định, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng;

c) Phối hợp với các tổ chức, cá nhân 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 cán bộ, công chức, viên chức và người lao động trong các cơ quan, đơn vị:

a) Nghiêm túc chấp hành Nội quy này và các quy định khác của pháp luật

về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao;

b) Khi tham gia vận hành mạng máy tính của cơ quan phải nghiêm chỉnh chấp hành chế độ bảo mật, an toàn, an ninh thông tin đồng thời chịu trách nhiệm đối với các thông tin mà mình cung cấp. Mỗi cán bộ, công chức, viên chức và người lao động phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp các thiết bị trên máy tính; không được vào các trang thông tin điện tử không rõ về nội dung; không tải và cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn; không nhấp chuột vào các đường dẫn lạ không rõ về nội dung; không cho phép bất cứ hành vi nào gây tổn hại đến dịch vụ, gây hư hỏng thiết bị mạng; không cung cấp thông tin không trung thực để công bố trên mạng; sử dụng mạng để thâm nhập vào các mạng máy tính khi chưa được phép; không đưa các thông tin có nội dung “mật”, “tối mật” và “tuyệt mật” lên hệ thống máy tính có kết nối mạng Internet;

c) Trong trao đổi thông tin, dữ liệu phục vụ công việc, các phòng, trạm, cán bộ, công chức, viên chức phải sử dụng hệ thống thông tin do cơ quan, đơn vị có thẩm quyền triển khai, như: Hệ thống thư điện tử tỉnh Lào Cai (@laocai.gov.vn) hoặc Hệ thống quản lý văn bản và điều hành (ioffice). Mỗi cán bộ, công chức, viên chức và người lao động không sử dụng các trang mạng xã hội, các dịch vụ thư điện tử công cộng,... để trao đổi thông tin quan trọng liên quan đến công việc chuyên môn của cơ quan, đơn vị;

d) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và công chức phụ trách công nghệ thông tin của đơn vị để kịp thời ngăn chặn và xử lý;

đ) Tham gia các chương trình đào tạo, hội nghị tập huấn về an toàn thông tin mạng do các cơ quan, đơn vị chuyên trách an toàn thông tin mạng hoặc Sở Thông tin và Truyền thông tổ chức.

Chương IV

TỔ CHỨC THỰC HIỆN

Điều 10. Khen thưởng, xử lý vi phạm

1. Công chức, viên chức và người lao động có thành tích xuất sắc trong bảo đảm an toàn, an ninh thông tin của Chi cục được khen thưởng theo quy định của pháp luật.

2. Công chức, viên chức và người lao động vi phạm các quy định của pháp luật về an toàn, an ninh thông tin tùy theo tính chất, mức độ vi phạm và hậu quả gây ra sẽ bị xử lý kỷ luật hành chính hoặc truy cứu trách nhiệm hình sự

theo quy định của pháp luật.

Điều 11. Trách nhiệm thi hành

Lãnh đạo, công chức, viên chức thuộc Chi cục Chăn nuôi và Thú y tỉnh Lào Cai có trách nhiệm triển khai thực hiện các quy định của pháp luật về an toàn, an ninh thông tin và Nội quy này.

Điều 12. Sửa đổi, bổ sung nội quy

Phòng Hành chính - Tổng hợp giúp Chi cục trưởng triển khai thực hiện Nội quy này; phối hợp với các phòng chuyên môn, các cá nhân có liên quan thường xuyên rà soát, đề xuất sửa đổi, bổ sung những nội dung không còn phù hợp đảm bảo thực hiện đúng quy định hiện hành về đảm bảo an toàn, an ninh thông tin./.