BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG
CỤC BẢO TỒN THIÊN NHIÊN VÀ ĐA DẠNG SINH HỌC

Số: 178 /QĐ-BTTN

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

Hà Nội, ngày 10 tháng 11 năm 2025

QUYẾT ĐỊNH

Ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Cục Bảo tồn thiên nhiên và Đa dạng sinh học

CỤC TRƯỞNG CỤC BẢO TỒN THIÊN NHIÊN VÀ ĐA DẠNG SINH HỌC

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

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 08 năm 2022 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 Quyết định số 1921/QĐ-BNNMT ngày 05 tháng 6 năm 2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường về việc Ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Bộ Nông nghiệp và Môi trường;

Căn cứ Quyết định số 215/QĐ-BNNMT ngày 01 tháng 3 năm 2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường về việc Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Cục Bảo tồn thiên nhiên và Đa dạng sinh học;

Căn cứ Tiêu chuẩn Việt Nam TCVN 11930:2017 Công nghệ thông tin – Các kỹ thuật an toàn – Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ;

Theo đề nghị của Giám đốc Trung tâm Điều tra, Quan trắc đa dạng sinh học.

QUYẾT ĐỊNH

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo đảm an toàn, an ninh thông tin mạng Cục Bảo tồn thiên nhiên và Đa dạng sinh học.

Điều 2. Quyết định này có hiệu lực từ ngày ký.

Điều 3. Chánh Văn phòng Cục; Giám đốc Trung tâm Điều tra, Quan trắc đa dạng sinh học; Thủ trưởng các đơn vị, công chức, viên chức, người lao động

trực thuộc Cục Bảo tồn thiên nhiên và Đa dạng sinh học và tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Thứ trưởng: Nguyễn Quốc Trị (để báo cáo);
- Cục trưởng: Bùi Chính Nghĩa (để báo cáo);
- Cục Chuyển đổi số (để phối hợp);
- Các Phó Cục trưởng: Dương Thanh An; Lê Văn Hữu; Hoàng Thị Thanh Nhàn;
- Các đơn vị trực thuộc Cục BTTN;
- Lưu: VT, ĐTQT.

KT. CỤC TRƯỞNG
PHÓ CỤC TRƯỞNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
CỤC BẢO TỒN THIÊN NHIÊN VÀ ĐA DẠNG SINH HỌC
BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG

Phan Việt Nga

BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG
CỤC BẢO TỒN THIÊN NHIÊN VÀ ĐA DẠNG SINH HỌC

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

QUY CHẾ
BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG, AN NINH MẠNG CỤC BẢO TỒN THIÊN NHIÊN VÀ ĐA DẠNG SINH HỌC

(Kèm theo Quyết định số /QĐ-BTTN ngày tháng năm 2025 của Cục trưởng Cục Bảo tồn thiên nhiên và Đa dạng sinh học)

CHƯƠNG I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

1. Quy chế này quy định các chính sách quản lý và các biện pháp nhằm bảo đảm an toàn, an ninh thông tin mạng trong các hoạt động chuyển đổi số, ứng dụng công nghệ thông tin (Sau đây gọi tắt là CNTT), vận hành, khai thác hệ thống, hạ tầng thông tin, phần mềm, dữ liệu thuộc phạm vi quản lý của Cục Bảo tồn thiên nhiên và Đa dạng sinh học (Sau đây gọi tắt là Cục BTTN) và các đơn vị trực thuộc Cục BTTN. Quy chế này không quy định đối với các thông tin mật, các quy định về bảo đảm an toàn thông tin (Sau đây gọi tắt là ATTT) mật thực hiện theo quy định hiện hành.

2. Phạm vi chính sách ATTT tại quy chế này, bao gồm:

a) Thiết lập chính sách ATTT.

b) Tổ chức bảo đảm ATTT.

c) Bảo đảm nguồn nhân lực.

d) Quản lý thiết kế, xây dựng hệ thống thông tin.

e) Quản lý vận hành hệ thống

Điều 2. Đối tượng áp dụng

1. Các đơn vị trực thuộc Cục BTTN và cán bộ, công chức, viên chức và người lao động thuộc các đơn vị trực thuộc Cục BTTN.

2. Cơ quan, tổ chức, cá nhân có kết nối vào hệ thống mạng của Cục BTTN.

3. Cơ quan, tổ chức, cá nhân cung cấp dịch vụ CNTT và ATTT mạng phục vụ hoạt động cho các đơn vị trực thuộc Cục BTTN.

Điều 3. Nguyên tắc chung về bảo đảm an toàn, an ninh thông tin mạng

1. Bảo đảm an toàn, an ninh thông tin là yêu cầu bắt buộc, thường xuyên, liên tục được nâng cao, cải tiến và phải bảo đảm an toàn, an ninh thông tin tuân thủ các nguyên tắc chung quy định tại Điều 4 Luật ATTT mạng và Điều 4 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 (Nghị định số 85/2016/NĐ-CP) và các quy định pháp luật khác có liên quan.

2. Cán bộ, công chức, viên chức và người lao động trong các đơn vị trực thuộc Cục BTTN có trách nhiệm bảo đảm an toàn, an ninh thông tin trong phạm vi xử lý công việc của mình theo quy định của Nhà nước, Bộ Nông nghiệp và Môi trường (Bộ NN&MT) và Cục BTTN.

3. Xử lý sự cố ATTT phải phù hợp với trách nhiệm, quyền hạn và bảo đảm lợi ích hợp pháp của cơ quan, đơn vị, cá nhân liên quan và theo quy định của pháp luật.

4. Việc bảo đảm an toàn hệ thống thông tin được thực hiện một cách tổng thể, đồng bộ, tập trung trong việc đầu tư các giải pháp bảo vệ, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp.

Điều 4. Các hành vi bị nghiêm cấm

Tuân thủ theo Điều 4, Quyết định số 1921/QĐ-BNNMT ngày 05 tháng 6 năm 2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường về việc Ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Bộ Nông nghiệp và Môi trường.

CHƯƠNG II
QUY ĐỊNH VỀ BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG, AN NINH MẠNG

Điều 5. Quản lý trang thiết bị công nghệ thông tin

1. Giao, gắn trách nhiệm cho cá nhân hoặc tập thể quản lý, sử dụng trang thiết bị CNTT.

2. Thực hiện các quy định, quy tắc trong quá trình sử dụng, giữ gìn bảo vệ trang thiết bị CNTT trong các trường hợp: cài đặt và cấu hình, bảo dưỡng, sửa chữa, mang ra khỏi cơ quan.

3. Trang thiết bị CNTT có lưu trữ dữ liệu nhạy cảm khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó, đảm bảo không có khả năng phục hồi. Trường hợp không thể xóa, tiêu hủy được dữ liệu, đơn vị bắt buộc phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên trang thiết bị CNTT đó.

4. Các thiết bị CNTT khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài hoặc ngừng sử dụng phải tháo bộ phận lưu trữ khỏi thiết bị hoặc xóa thông tin, dữ liệu lưu trữ trên thiết bị.

5. Trung tâm Điều tra, Quan trắc đa dạng sinh học được phân công quản lý, vận hành hạ tầng CNTT có trách nhiệm xây dựng quy trình bảo dưỡng, bảo trì và hướng dẫn cách sử dụng, quản lý, vận hành hệ thống hạ tầng kỹ thuật của mình;

chỉ định bộ phận chuyên trách về CNTT thực hiện quản lý, vận hành và định kỳ kiểm tra, sửa chữa, bảo trì thiết bị.

Điều 6. Quy định đối với cán bộ, công chức, viên chức và người lao động trong việc đảm bảo an toàn, an ninh thông tin

1. Tuân thủ các hành vi nghiêm cấm tại Điều 4 Quy định này.

2. Tuân thủ theo Điều 14 tại Quyết định số 1921/QĐ-BNNMT ngày 05 tháng 6 năm 2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường về việc Ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Bộ Nông nghiệp và Môi trường.

Điều 7. Quản lý an toàn vận hành hệ thống công nghệ thông tin

1. Quản lý ATTT đối với phòng máy chủ

Tuân thủ theo các quy định tại Điều 9 Quyết định số 1921/QĐ-BNNMT ngày 05 tháng 6 năm 2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường về việc Ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Bộ Nông nghiệp và Môi trường.

2. Quản lý ATTT khi sử dụng máy tính

a) Cá nhân chỉ cài đặt phần mềm hợp lệ và thuộc danh mục phần mềm được phép sử dụng do cơ quan có thẩm quyền ban hành trên máy tính được đơn vị cấp cho mình; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận chuyên trách về CNTT; thường xuyên cập nhật phần mềm và hệ điều hành.

b) Cài đặt phần mềm xử lý phần mềm độc hại và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy tính phải tắt máy và thông báo trực tiếp đến phòng Cơ sở dữ liệu đa dạng sinh học -Trung tâm Điều tra, Quan trắc đa dạng sinh học là đơn vị chuyên trách về CNTT để được xử lý kịp thời.

c) Chỉ truy nhập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; có trách nhiệm bảo mật tài khoản truy nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác.

3. Quản lý ATTT đối với hệ thống mạng máy tính

a) Hệ thống mạng nội bộ (LAN) phải được thiết kế phân vùng theo các chính sách ATTT riêng, bao gồm: vùng mạng người dùng; vùng mạng kết nối hệ thống ra bên ngoài Internet và các mạng khác; vùng máy chủ công cộng; vùng máy chủ nội bộ; vùng máy chủ quản trị. Dữ liệu trao đổi giữa các vùng phải được quản lý, giám sát bởi hệ thống các thiết bị mạng, thiết bị bảo mật.

b) Đơn vị trực thuộc Cục BTTN khi tham gia kết nối, sử dụng hệ thống mạng diện rộng (WAN) của Bộ Nông nghiệp và Môi trường có trách nhiệm đảm bảo ATTT đối với hệ thống mạng nội bộ và các thiết bị của mình khi thực hiện

kết nối vào mạng diện rộng; thông báo sự cố hoặc các hành vi phá hoại, xâm nhập về Trung tâm Hạ tầng số - Cục Chuyển đổi số để xử lý; không được tiết lộ tên đăng ký, mật khẩu, tiện ích, tệp hỗ trợ và các cách thức khác… để truy nhập vào hệ thống mạng diện rộng cho tổ chức, cá nhân khác; Không được tìm cách truy nhập dưới bất cứ hình thức nào vào các khu vực không được phép truy nhập.

c) Trung tâm Điều tra, Quan trắc đa dạng sinh học được giao quản trị hệ thống thông tin phải áp dụng các biện pháp kỹ thuật cần thiết bảo đảm ATTT trong hoạt động kết nối Internet, tối thiểu đáp ứng các yêu cầu kết nối đồng thời, hỗ trợ các công nghệ riêng ảo thông dụng và có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ (DdoS); Lọc, bỏ, không cho phép truy cập các trang tin có nghi ngờ chứa mã độc hoặc nội dung không phù hợp.

d) Các đường truyền dữ liệu, đường truyền Internet và các hệ thống dây dẫn các mạng LAN, WAN cần phải được lắp đặt trong ống, máng che đậy kín hoặc phải có giải pháp phù hợp nhằm hạn chế khả năng tiếp cận trái phép. Ngắt kết nối cổng Ethernet không sử dụng, đặc biệt là ở khu vực làm việc chung của các đơn vị.

e) Mạng không dây (wifi) của các đơn vị trực thuộc Cục phải được đặt mật khẩu và cài đặt cơ chế giám sát người dùng khi truy cập.

4. Quản lý tài khoản truy cập

a) Tuân thủ các quy định tại Điều 11 Quyết định số 1921/QĐ-BNNMT ngày 05 tháng 6 năm 2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường về việc Ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Bộ Nông nghiệp và Môi trường.

b) Các hệ thống thông tin cần giới hạn số lần đăng nhập sai liên tiếp vào hệ thống. Hệ thống tự động khóa tài khoản trong một khoảng thời gian nhất định nếu liên tục đăng nhập sai vượt quá số lần quy định trước khi tiếp tục cho đăng nhập và có phương thức hỗ trợ cấp lại mật khẩu tài khoản.

5. Quản lý máy chủ và ứng dụng

a) Phải được đặt trong các vùng mạng dành riêng cho máy chủ, tối thiểu gồm vùng mạng máy chủ công cộng, vùng mạng máy chủ nội bộ và vùng mạng máy chủ quản trị;

b) Chỉ cho phép kết nối đến những dịch vụ cần thiết trên Internet; chỉ mở và cung cấp các dịch vụ cần thiết ra Internet;

c) Chỉ cài đặt và sử dụng các phần mềm đúng bản quyền, nguồn gốc rõ ràng, thực sự cần thiết. Không sử dụng các phần mềm đã được cảnh báo không an toàn hoặc không được nhà sản xuất hỗ trợ kỹ thuật khi không thực sự cần thiết;

d) Triển khai các biện pháp sao lưu dự phòng để nâng cao khả năng phục hồi hoạt động khi xảy ra sự cố; Phải lưu trữ dữ liệu sao lưu ở nơi an toàn, không

cùng phân vùng lưu trữ các ứng dụng và được kiểm tra thường xuyên, bảo đảm sẵn sàng cho việc sử dụng khi cần thiết.

e) Giám sát thường xuyên, liên tục để phát hiện và cảnh báo sớm nguy cơ mất an toàn thông tin.

f) Yêu cầu về bảo đảm an toàn thông tin phải được đưa vào tất cả các công đoạn thiết kế, xây dựng, triển khai và vận hành, sử dụng phần mềm, ứng dụng.

g) Phần mềm, ứng dụng phải đáp ứng các yêu cầu sau: cấu hình phần mềm, ứng dụng để xác thực người sử dụng; giới hạn số lần đăng nhập sai liên tiếp; giới hạn thời gian để chờ đóng phiên kết nối; mã hóa thông tin xác thực trên hệ thống; không khuyến khích việc đăng nhập tự động.

h) Thiết lập, phân quyền truy cập, quản trị, sử dụng tài nguyên khác nhau của phần mềm, ứng dụng với người sử dụng/nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau; tách biệt cổng giao tiếp quản trị phần mềm ứng dụng với cổng giao tiếp cung cấp dịch vụ; đóng các cổng giao tiếp không sử dụng.

i) Chỉ cho phép sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin như SSH, SSL, VPN hoặc tương đương khi truy cập, quản trị phần mềm, ứng dụng từ xa trên môi trường mạng; hạn chế truy cập đến mã nguồn của phần mềm, ứng dụng và phải đặt mã nguồn trong môi trường an toàn do bộ phận chuyên trách công nghệ thông tin quản lý.

j) Ghi và lưu giữ bản ghi nhật ký hệ thống (log files) của phần mềm, ứng dụng trong khoảng thời gian tối thiểu 03 tháng với những thông tin cơ bản: thời gian, địa chỉ, tài khoản (nếu có), nội dung truy cập và sử dụng phần mềm, ứng dụng; các lỗi phát sinh trong quá trình hoạt động; thông tin đăng nhập khi quản trị.

k) Phần mềm, ứng dụng cần kiểm tra phát hiện và khắc phục các điểm yếu về an toàn, an ninh thông tin trước khi đưa vào sử dụng và trong quá trình sử dụng.

l) Thực hiện quy trình kiểm soát cài đặt, cập nhật, vá lỗi bảo mật phần mềm, ứng dụng trên các máy chủ, máy tính cá nhân, thiết bị kết nối mạng đang hoạt động thuộc hệ thống mạng nội bộ

6. Quản lý phòng chống phần mềm độc hại

a) Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống phần mềm độc hại. Các phần mềm phòng chống phần mềm độc hại phải được thiết lập chế độ tự động cập nhật, tự động quét và diệt phần mềm độc hại.

b) Hệ điều hành, phần mềm cài đặt trên máy chủ, máy trạm phải được cập nhật vá lỗ hổng bảo mật thường xuyên, kịp thời.

c) Khi gửi văn bản điện tử gửi qua hệ thống thư điện tử phải có định dạng theo Danh mục tiêu chuẩn kỹ thuật về ứng dụng CNTT trong cơ quan nhà nước như: (.txt), (.doc), (.odt), (pdf) và các định dạng khác theo quy định, không được gửi các file thực thi (.com), (.bat)…

d) Cán bộ, công chức, viên chức và người lao động phải được hướng dẫn về phòng chống mã độc, các rủi ro do mã độc gây ra; không được tự ý gỡ bỏ các phần mềm phòng chống phần mềm độc hại trên máy tính khi chưa có sự đồng ý của người có thẩm quyền trong cơ quan.

e) Tất cả các máy tính của đơn vị phải được cấu hình vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động.

f) Các máy tính xách tay, thiết bị di động (điện thoại thông minh, máy tính bảng...) trước khi kết nối vào mạng LAN nội bộ của cơ quan, đơn vị phải bảo đảm đã được cài chương trình phòng chống phần mềm độc hại và đã được kiểm duyệt về các phần mềm độc hại.

g) Tất cả các tập tin, thư mục trên các thiết bị di động (USB, đĩa cứng di động…) phải được quét phần mềm độc hại trước khi sao chép vào máy tính sử dụng.

h) Máy chủ chỉ được dùng để cài đặt các phần mềm, dịch vụ dùng chung của cơ quan, đơn vị; không cài đặt phần mềm không rõ nguồn gốc, phần mềm phục vụ mục đích cá nhân và mục đích khác, không phục vụ công việc.

i) Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại trên máy trạm như: máy hoạt động chậm bất thường; cảnh báo từ phần mềm phòng chống phần mềm độc hại, tình trạng này lặp đi lặp lại nhiều lần, ở các vị trí khác nhau; quan trọng nhất là có dấu hiệu mất dữ liệu... người sử dụng phải tắt máy, ngắt kết nối từ máy tính đến mạng LAN nội bộ, mạng WAN nội bộ, mạng Internet... và báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.

j) Định kỳ hàng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; Thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.

7. Bảo đảm an toàn trong thiết kế, xây dựng hệ thống thông tin

a) Các hoạt động liên quan đến xây dựng, thiết lập, quản lý, vận hành, nâng cấp mở rộng hệ thống thông tin phải thực hiện xác định cấp độ và phương án bảo đảm ATTT mạng theo Quy định tại Nghị định số 85/2016/NĐ-CP và Thông tư 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 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" (Thông tư 12/2022/TT-BTTTT); Quy chế ATTT của Bộ Nông nghiệp và Môi trường và phải tuân thủ Khung kiến trúc Chính phủ điện tử Việt Nam.

b) Nhiệm vụ quản lý về hướng dẫn xác định hệ thống thông tin và cấp độ an toàn hệ thống thông tin; thực hiện các yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ; thực hiện kiểm tra, đánh giá ATTT mạng; tiếp nhận và thẩm định

hồ sơ đề xuất cấp độ; báo cáo, chia sẻ thông tin thực hiện theo quy định tại Thông tư số 12/2022/TT-BTTTT.

c) Cơ quan, đơn vị chủ quản hệ thống thông tin phải tổ chức kiểm tra, đánh giá định kỳ về an toàn thông tin của các hệ thống thông tin đang quản lý.

8. Phát triển phần mềm theo hình thức thuê khoán.

a) Có điều khoản hợp đồng và các cam kết đối với bên thuê khoán khi thực hiện các nội dung liên quan đến việc phát triển phần mềm thuê khoán.

b) Các nhà phát triển phải cung cấp đầy đủ mã nguồn phần mềm.

c) Phần mềm thuê khoán phải được kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.

d) Phần mềm thuê khoán phải được kiểm tra, đánh giá ATTT trước khi đưa vào sử dụng.

9. Quản lý an toàn người sử dụng đầu cuối

a) Kết nối máy tính, thiết bị đầu cuối của người sử dụng vào hệ thống.

- Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm ATTT và các quy định khác của cơ quan.

- Khi cài đặt, kết nối máy tính, thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của bộ phận chuyên trách về ATTT.

- Máy tính, thiết bị đầu cuối phải được xử lý điểm yếu ATTT, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống.

b) Trong quá trình sử dụng.

- Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về ATTT mạng. Chịu trách nhiệm bảo đảm ATTT mạng trong phạm vi trách nhiệm và quyền hạn được giao.

- Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao.

- Khi phát hiện nguy cơ hoặc sự cố mất ATTT mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách CNTT của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý.

- Tham gia các chương trình đào tạo, hội nghị về ATTT mạng được các đơn vị chuyên môn tổ chức.

10. Bảo đảm ATTT mức dữ liệu

Tuân thủ theo các quy định tại Điều 13 Quyết định số 1921/QĐ-BNNMT ngày 05 tháng 6 năm 2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường về việc Ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Bộ Nông nghiệp và Môi trường.

Điều 8. Xác định cấp độ và phương án bảo đảm an toàn hệ thống thông tin

1. Việc xác định cấp độ hệ thống thông tin và xây dựng phương án bảo vệ hệ thống thông tin theo cấp độ phục vụ mục đích đánh giá ATTT và bảo đảm ATTT cho các hệ thống thông tin. Nguyên tắc bảo đảm ATTT theo cấp độ và nguyên tắc xác định cấp độ căn cứ trên các nguyên tắc quy định tại Điều 4, Điều 5 Nghị định số 85/2016/NĐ-CP.

2. Đơn vị vận hành hệ thống thông tin

a) Trung tâm Điều tra, Quan trắc đa dạng sinh học là đơn vị vận hành các hệ thống thông tin, cơ sở dữ liệu dùng chung của Cục BTTN và các hệ thống thông tin, cơ sở dữ liệu chuyên ngành khác được giao quản lý, vận hành.

b) Các hệ thống thông tin trước khi đưa vào khai thác, sử dụng phải được giao cho đơn vị quản lý, vận hành theo quy định tại Điều 5, Thông tư số 12/2022/TT-BTTTT.

4. Đơn vị chuyên trách về ATTT

a) Phòng Cơ sở dữ liệu đa dạng sinh học thuộc Trung tâm Điều tra, quan trắc đa dạng sinh học là đơn vị chuyên trách về ATTT của Cục.

b) Phòng Cơ sở dữ liệu đa dạng sinh học bố trí cán bộ chuyên trách để đảm bảo ATTT.

5. Thẩm định xác định cấp độ an toàn hệ thống thông tin.

a) Đơn vị lập hồ sơ đề xuất cấp độ: Đối với các hệ thống thông tin thuộc các nhiệm vụ, dự án đang trong giai đoạn lập dự án, đơn vị lập dự án lập hồ sơ đề xuất cấp độ; đối với các hệ thống thông tin thuê dịch vụ, đơn vị chủ trì thuê dịch vụ lập hồ sơ đề xuất cấp độ; đối với các hệ thống thông tin đang trong giai đoạn triển khai, đơn vị chủ trì triển khai lập hồ sơ đề xuất cấp độ; đối với các hệ thống thông tin đang vận hành, đơn vị vận hành lập hồ sơ đề xuất cấp độ.

b) Đối với các hệ thống thông tin được đề xuất từ cấp độ 3 trở lên, đơn vị được giao quản lý hệ thống thông tin của Cục phối hợp cùng Trung tâm Điều tra, Quan trắc đa dạng sinh học gửi xin ý kiến chuyên môn của Cục Chuyển đổi số trước khi trình các cấp có thẩm quyền thẩm định, phê duyệt cấp độ.

c) Thẩm quyền thẩm định và phê duyệt cấp độ theo quy định tại Điều 12 Nghị định số 85/2016/NĐ-CP.

6. Trình tự, thủ tục xác định cấp độ hệ thống thông tin

Tuân thủ theo các quy định tại Điều 6 Quyết định số 1921/QĐ-BNNMT ngày 05 tháng 6 năm 2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường về việc Ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Bộ Nông nghiệp và Môi trường.

7. Phương án bảo đảm an toàn hệ thống thông tin.

a) Phương án bảo đảm an toàn hệ thống thông tin phải phù hợp với cấp độ của hệ thống thông tin và đáp ứng yêu cầu quy định tại Thông tư số 12/2022/TT-

BTTTT, phù hợp với tiêu chuẩn TCVN 11930:2017, các tiêu chuẩn, quy chuẩn kỹ thuật khác và chính sách ATTT mạng của Bộ NN&MT.

b) Trung tâm Điều tra, Quan trắc đa dạng sinh học tổ chức triển khai phương án bảo đảm an toàn hệ thống thông tin sau khi hồ sơ đề xuất cấp độ hoặc phương án bảo đảm an toàn hệ thống được phê duyệt.

c) Phòng Cơ sở dữ liệu đa dạng sinh học thuộc Trung tâm Điều tra, quan trắc đa dạng sinh học chuyên trách về ATTT chịu trách nhiệm giám sát việc triển khai các phương án bảo đảm ATTT đã được phê duyệt.

Điều 9. Bảo đảm an toàn thông tin khi tiếp nhận, phát triển, vận hành và bảo trì hệ thống thông tin

Tuân thủ theo các quy định tại Điều 8 Quyết định số 1921/QĐ-BNNMT ngày 05 tháng 6 năm 2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường về việc Ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Bộ Nông nghiệp và Môi trường.

Điều 10. Quản lý thuê dịch vụ công nghệ thông tin

1. Khi ký kết hợp đồng dịch vụ CNTT, cơ quan, đơn vị sử dụng dịch vụ phải xác định rõ phạm vi, trách nhiệm, quyền hạn và nghĩa vụ của các bên liên quan về bảo đảm ATTT. Trong hợp đồng phải bao gồm các điều khoản về việc xử lý vi phạm quy định bảo đảm ATTT và trách nhiệm bồi thường thiệt hại do hành vi vi phạm của bên cung cấp dịch vụ gây ra.

2. Trách nhiệm của cơ quan, đơn vị trong quá trình sử dụng dịch vụ CNTT.

a) Quản lý thông tin, dữ liệu phát sinh từ dịch vụ đó, không để bên cung cấp dịch vụ truy nhập, sử dụng thông tin, dữ liệu thuộc phạm vi Nhà nước quản lý.

b) Yêu cầu bên cung cấp dịch vụ phải bảo mật thông tin, dữ liệu, mã nguồn, tài liệu thiết kế; triển khai các biện pháp bảo đảm ATTT theo quy định tại Quy chế này, Luật ATTT mạng và các quy định khác có liên quan.

c) Giám sát chặt chẽ và giới hạn quyền truy cập của bên cung cấp dịch vụ khi cho phép truy cập vào hệ thống thông tin của cơ quan, đơn vị.

3. Trách nhiệm của cơ quan, đơn vị khi phát hiện bên cung cấp dịch vụ có dấu hiệu vi phạm quy định bảo đảm ATTT.

a) Tạm dừng hoặc đình chỉ hoạt động của bên cung cấp dịch vụ tùy theo mức độ vi phạm.

b) Thông báo chính thức các hành vi vi phạm của bên cung cấp dịch vụ.

c) Thu hồi ngay lập tức quyền truy cập hệ thống thông tin đã cấp cho bên cung cấp dịch vụ.

d) Kiểm tra, xác định, lập báo cáo mức độ vi phạm và thiệt hại xảy ra; thông báo cho bên cung cấp dịch vụ và tiến hành các thủ tục xử lý vi phạm và bồi thường thiệt hại.

4. Trách nhiệm của cơ quan, đơn vị khi kết thúc sử dụng dịch vụ.

a) Thu hồi quyền truy cập hệ thống thông tin và các tài sản khác liên quan đã cấp cho bên cung cấp dịch vụ; thay đổi các khóa, mật khẩu truy cập hệ thống thông tin.

b) Yêu cầu bên cung cấp dịch vụ chuyển giao đầy đủ các thông tin, dữ liệu, mã nguồn, tài liệu thiết kế và các công cụ cần thiết để bảo đảm cơ quan, đơn vị vẫn có thể khai thác sử dụng dịch vụ được liên tục kể cả trong trường hợp thay đổi bên cung cấp dịch vụ.

Điều 11. Giám sát an toàn, an ninh thông tin mạng

1. Tuân thủ theo các quy định tại khoản 1, khoản 2, khoản 3 và khoản 4 Điều 15 Quyết định số 1921/QĐ-BNNMT ngày 05 tháng 6 năm 2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường về việc Ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Bộ Nông nghiệp và Môi trường.

2. Trung tâm Điều tra, Quan trắc đa dạng sinh học được giao quản trị hệ thống thông tin trực thuộc Cục phân công Phòng Cơ sở dữ liệu đa dạng sinh học làm đầu mối giám sát ATTT mạng để tiếp nhận cảnh báo, cung cấp, trao đổi, chia sẻ thông tin với Cục Chuyển đổi số trong các hoạt động giám sát ATTT tại đơn vị và tại Cục.

Điều 12. Kiểm tra, đánh giá an toàn thông tin

1. Tuân thủ các quy định tại khoản 1, khoản 2, khoản 3, khoản 4 tại Điều 16 Quyết định số 1921/QĐ-BNNMT ngày 05 tháng 6 năm 2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường về việc Ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Bộ Nông nghiệp và Môi trường.

2. Trung tâm Điều tra, Quan trắc đa dạng sinh học thực hiện kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ tại Cục theo quy định tại Điều 11 và Điều 12 của Thông tư 12/2022/TT-BTTTT.

3. Trung tâm Điều tra, Quan trắc đa dạng sinh học là đơn vị chuyên trách về ATTT của Cục, thực hiện việc đánh giá hiệu quả của các biện pháp bảo đảm ATTT theo thẩm quyền. Nội dung đánh giá là cơ sở để điều chỉnh phương án bảo đảm ATTT cho phù hợp.

Điều 13. Ứng cứu sự cố an toàn thông tin mạng

1. Nguyên tắc ứng cứu xử lý sự cố

a) Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả.

b) Phối hợp chặt chẽ, tuân thủ quy định của pháp luật về điều phối ứng cứu sự cố ATTT.

c) Ứng cứu xử lý sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin.

d) Việc xử lý sự cố ATTT phải bảo đảm quyền và lợi ích hợp pháp của cơ quan, đơn vị; cá nhân, bảo mật thông tin cá nhân, thông tin riêng của cơ quan, đơn vị khi tham gia các hoạt động ứng cứu xử lý sự cố.

2. Kế hoạch ứng phó sự cố bảo đảm ATTT mạng

a) Trung tâm Điều tra, Quan trắc đa dạng sinh học phối hợp cùng các đơn vị xây dựng kế hoạch ứng phó sự cố cho các hệ thống thông tin do đơn vị trực tiếp quản lý, báo cáo Cục trưởng xem xét, quyết định và tổ chức triển khai sau khi phê duyệt. Đối với các nội dung trong kế hoạch vượt thẩm quyền quyết định của đơn vị, đơn vị lấy ý kiến của Cục Chuyển đổi số.

b) Kế hoạch ứng phó sự cố được rà soát và điều chỉnh hàng năm cho phù hợp, làm cơ sở để xây dựng kế hoạch bảo đảm an toàn, an ninh thông tin năm tiếp theo.

3. Phân loại sự cố ATTT

a) 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.

b) Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật.

c) Sự cố do lỗi của công chức, viên chức quản trị, vận hành hệ thống.

d) Sự cố do các thảm họa tự nhiên.

3. Phân loại mức độ nghiêm trọng sự cố

Phân loại mức độ nghiêm trọng của sự cố được chia thành 04 cấp, gồm:

Thấp: sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan, đơn vị như: máy tính trạm bị nhiễm phần mềm độc hại; phần mềm hệ điều hành, các phần mềm ứng dụng cài đặt trên máy tính cá nhân phát sinh lỗi.

Trung bình: sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của đơn vị như: hệ thống mạng của 01 phòng, ban thuộc đơn vị bị ngưng hoạt động, phần mềm độc hại lây nhiễm tất cả các máy tính trạm trong 01 phòng, ban.

Cao: sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến một trong các hoạt động chính của cơ quan như: hệ thống quản lý văn bản và điều hành, hồ sơ cấp phép, một cửa điện tử của đơn vị bị ngưng hoạt động, một số thiết bị CNTT quan trọng (bộ chuyển mạch trung tâm, thiết bị định tuyến, thiết bị tường lửa, máy chủ quản lý tập tin chung,) bị hư hỏng.

Khẩn cấp/Nghiêm trọng: sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của cơ quan, đơn vị như: toàn bộ hệ thống thiết bị CNTT, hệ thống

cung cấp điện ngừng hoạt động, hệ thống trang thông tin điện tử bị tin tặc (hacker) tấn công, xâm nhập, thay đổi nội dung...

4. Quy trình ứng cứu sự cố ATTT

Bước 1: Nếu hệ thống có nguy cơ mất ATTT mạng thuộc thẩm quyền cơ quan, đơn vị trực tiếp quản lý thì thực hiện tiếp Bước 2. Nếu hệ thống thông tin có nguy cơ mất ATTT mạng không thuộc đơn vị trực tiếp quản lý thì thực hiện Bước 3.

Bước 2: Tiến hành xử lý sự cố theo quy chế nội bộ của cơ quan, đơn vị. Nếu sự cố được khắc phục thì lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố. Khi sự cố vượt quá khả năng xử lý của cơ quan, lập biên bản ghi nhận và thực hiện tiếp Bước 3.

Bước 3: Báo sự cố đến đơn vị chuyên trách về ATTT của Cục: Trung tâm Điều tra, Quan trắc đa dạng sinh học theo mẫu số 03 của 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 ATTT trên toàn quốc (Thông tư số 20/2017/TT-BTTTT) và thực hiện tiếp Bước 4.

Bước 4: Phối hợp với Trung tâm Điều tra, Quan trắc đa dạng sinh học và các cơ quan, tổ chức có liên quan để tiến hành khắc phục sự cố và thực hiện Bước 5. Trong trường hợp nằm ngoài khả năng xử lý của Trung tâm Điều tra, Quan trắc đa dạng sinh học thì Trung tâm phối hợp cùng đơn vị gửi báo cáo sự cố đến lãnh đạo cơ quan, đơn vị và các đơn vị ứng cứu sự cố cấp trên để xử lý và thực hiện lại Bước 4.

Bước 5: Lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố theo mẫu số 04 của Thông tư số 20/2017/TT-BTTTT, lãnh đạo cơ quan, đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại, báo cáo bằng văn bản cho cơ quan cấp trên trực tiếp quản lý.

5. Diễn tập ứng cứu sự cố ATTT

Trung tâm Điều tra, Quan trắc đa dạng sinh học phối hợp cùng các đơn vị trong Cục tham gia diễn tập ứng cứu sự cố ATTT mạng do Cục Chuyển đổi số chủ trì.

Điều 14. Đào tạo, bồi dưỡng nghiệp vụ, tuyên truyền, phổ biến nâng cao nhận thức và tăng cường năng lực ứng cứu, xử lý sự cố về an toàn thông tin

1. Các đơn vị trực thuộc Cục BTTN xác định nhu cầu về đào tạo nguồn nhân lực bảo đảm ATTT tại đơn vị mình gửi Trung tâm Điều tra, Quan trắc đa dạng sinh học để tổng hợp báo cáo Lãnh đạo Cục gửi Cục Chuyển đổi số.

2. Trung tâm Điều tra, Quan trắc đa dạng sinh học chủ động phối hợp với các đơn vị chuyên môn tổ chức đào tạo, bồi dưỡng nghiệp vụ về ATTT, sử dụng máy tính cho các cán bộ của Cục BTTN.

3. Các đơn vị trực thuộc Cục BTTN thường xuyên 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 tại đơn vị

CHƯƠNG III
TRÁCH NHIỆM CỦA CÁC TỔ CHỨC LIÊN QUAN

Điều 15. Trách nhiệm của Trung tâm Điều tra, Quan trắc đa dạng sinh học

1. Thực hiện các trách nhiệm được giao tại Quy chế này. Là đơn vị chuyên trách về CNTT của Cục BTTN, giúp Lãnh đạo Cục thực hiện quản lý ATTT trong các hoạt động ứng dụng CNTT, chuyển đổi số của Bộ Nông nghiệp và Môi trường theo quy định của Quy chế này và các quy định khác của pháp luật có liên quan.

2. Hướng dẫn triển khai Quy chế này và các quy định liên quan về an toàn, an ninh thông tin mạng.

3. Thường xuyên tổ chức các hoạt động tuyên truyền, nâng cao nhận thức về bảo đảm an toàn, an ninh thông tin; nhận diện, cảnh giác, phòng ngừa và ngăn chặn các hoạt động vi phạm pháp luật trên không gian mạng đến toàn thể cán bộ, công chức, viên chức và người lao động tại đơn vị. Định kỳ báo cáo Lãnh đạo Cục về thông tin, tình hình thực hiện. Phối hợp cùng các đơn vị xây dựng và triển khai kế hoạch về an toàn, an ninh thông tin mạng của Cục.

4. Bảo đảm an toàn, an ninh thông tin cho các hệ thống thông tin, cơ sở dữ liệu chuyên ngành về bảo tồn thiên nhiên, đa dạng sinh học của Cục. Tùy theo mức độ của sự số, phối hợp với Cục Chuyển đổi số và các cơ quan chức năng ứng cứu các sự cố mất ATTT.

Điều 16. Trách nhiệm của các đơn vị trực thuộc Cục Bảo tồn thiên nhiên và Đa dạng sinh học

1. Thực hiện các trách nhiệm được giao tại Quy chế này. Tổ chức triển khai thực hiện Quy chế này tại đơn vị và phối hợp với Trung tâm Điều tra, Quan trắc đa dạng sinh học thực hiện bảo đảm ATTT, an ninh mạng cho các hệ thống thông tin, cơ sở dữ liệu dùng chung của Cục và các hệ thống thông tin do đơn vị quản lý, vận hành. Chịu trách nhiệm trước Lãnh đạo Cục trong công tác bảo đảm ATTT mạng của đơn vị mình.

2. Thực hiện các báo cáo theo quy định, gửi Trung tâm Điều tra, Quan trắc đa dạng sinh học để tổng hợp, báo cáo Lãnh đạo Cục và các đơn vị cơ quan nhà nước chuyên trách về ATTT.

3. Triển khai thực hiện Quy chế/Nội quy bảo đảm an toàn, an ninh thông tin mạng tại đơn vị bảo đảm phù hợp với Quy chế này.

4. Các đơn vị thực hiện việc quản lý trang thiết bị CNTT và cán bộ, công chức, viên chức, người lao động theo Điều 6 và Điều 7 của Quy chế này.

Điều 17. Trách nhiệm của cán bộ, công chức, viên chức và người lao động trong đơn vị trực thuộc Cục

1. Trách nhiệm của cán bộ, công chức, viên chức phụ trách ATTT mạng.

a) Chịu trách nhiệm bảo đảm ATTT mạng khi sử dụng internet kết nối tại đơn vị.

b) Tham mưu lãnh đạo cơ quan, đơn vị ban hành các quy định, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm ATTT mạng.

c) Thực hiện việc giám sát, đánh giá, báo cáo thủ trưởng cơ quan, đơn vị các rủi ro mất ATTT mạng và mức độ nghiêm trọng của các rủi ro đó.

d) 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 đơn vị.

a) Nghiêm túc chấp hành các quy định, quy trình nội bộ, Quy chế này và các quy định khác của pháp luật về ATTT mạng. Chịu trách nhiệm bảo đảm ATTT mạng trong phạm vi trách nhiệm và quyền hạn được giao.

b) Khi tham gia vận hành mạng máy tính của cơ quan, đơn vị, 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 cơ quan, đơn vị, 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 của bộ, ngành, lĩnh vực; hệ thống quản lý văn bản và điều hành. 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 ATTT mạng phải báo cáo ngay với cấp trên và bộ phận chuyên trách CNTT của đơn vị để kịp thời ngăn chặn và xử lý.

e) Tham gia các chương trình đào tạo, hội nghị về ATTT mạng do các cơ quan, đơn vị chuyên trách ATTT mạng hoặc Bộ Công an tổ chức.

3. Thủ trưởng các đơn vị trực thuộc Cục phổ biến tới cán bộ, công chức, viên chức, người lao động của đơn vị; thường xuyên kiểm tra việc thực hiện Quy chế này tại đơn vị; chịu trách nhiệm về các vi phạm, thất thoát thông tin, dữ liệu quan trọng thuộc phạm vi quản lý của đơn vị.

4. Cán bộ, công chức, viên chức, người lao động của các đơn vị trực thuộc Cục có trách nhiệm tuân thủ Quy chế; thông báo các vấn đề bất thường liên quan tới ATTT cho Lãnh đạo đơn vị, bộ phận chuyên trách về ATTT mạng; chịu trách nhiệm trước pháp luật và Lãnh đạo đơn vị về các vi phạm, thất thoát dữ liệu quan trọng của ngành do không tuân thủ Quy chế.

Điều 18. Trách nhiệm của tổ chức, cá nhân khác

Các tổ chức, cá nhân khác có sử dụng các hệ thống thông tin cho Cục triển khai hoặc liên quan đến hoạt động ứng dụng CNTT của Cục phải tuân thủ Quy chế này và các quy định hiện hành của pháp luật có liên quan.

CHƯƠNG IV
TỔ CHỨC THỰC HIỆN

Điều 19. Kinh phí thực hiện

1. Kinh phí bảo đảm ATTT mạng và an ninh mạng được lấy từ nguồn ngân sách nhà nước có trong dự toán hàng năm của Cục và từ nguồn kinh phí hợp lý khác.

2. Căn cứ vào kế hoạch hàng năm, các đơn vị liên quan có trách nhiệm xây dựng kế hoạch, đề xuất dự toán cho các hoạt động bảo đảm ATTT mạng, an ninh thông tin mạng tại đơn vị gửi Trung tâm Điều tra, Quan trắc đa dạng sinh học tổng hợp, gửi Văn phòng Cục thẩm định, trình Lãnh đạo Cục xem xét phê duyệt.

Điều 20. Công tác kiểm tra

1. Các đơn vị trực thuộc Cục thường xuyên kiểm tra, theo dõi và đánh giá công tác bảo đảm an toàn, an ninh thông tin mạng tại cơ quan, đơn vị mình.

2. Giao Trung tâm Điều tra, Quan trắc đa dạng sinh học kiểm tra và báo cáo Lãnh đạo Cục việc thực hiện Quy chế này tại các đơn vị trực thuộc.

Điều 21. Chế độ báo cáo an toàn, an ninh thông tin mạng

1. Tuân thủ các quy định tại Điều 19 Quyết định số 1921/QĐ- BNNMT ngày 05 tháng 6 năm 2025 của Bộ trưởng Bộ Nông nghiệp và Môi trường về việc Ban hành Quy chế bảo đảm an toàn thông tin mạng, an ninh mạng Bộ Nông nghiệp và Môi trường.

2. Trách nhiệm lập báo cáo, gửi và phê duyệt báo cáo

Trung tâm Điều tra, Quan trắc đa dạng sinh học có trách nhiệm xây dựng các báo cáo trình Lãnh đạo Cục phê duyệt, gửi Cục Chuyển đổi số để tổng hợp và báo cáo Lãnh đạo Bộ.

Điều 22. Khen thưởng, xử lý vi phạm

1. Giao Trung tâm Điều tra, Quan trắc đa dạng sinh học tiến hành kiểm tra, đánh giá, xếp hạng ATTT, trên cơ sở đó tham mưu, đề xuất Lãnh đạo khen thưởng đơn vị và cá nhân thực hiện tốt Quy chế này hằng năm theo quy định.

2. Đơn vị hoặc cá nhân vi phạm Quy chế này, tùy theo tính chất, mức độ vi phạm có thể bị xử lý hành chính, xử lý kỷ luật hoặc các hình thức xử lý khác theo quy định hiện hành; nếu vi phạm gây thiệt hại lớn đến tài nguyên thông tin của Bộ thì phải chịu trách nhiệm về những thiệt hại gây ra theo quy định của pháp luật.

3. Việc giải quyết khiếu nại, tố cáo và tranh chấp được thực hiện theo quy định liên quan của pháp luật.

Điều 23. Trách nhiệm thi hành

1. Thủ trưởng các đơn vị trực thuộc Cục có trách nhiệm phổ biến, quán triệt đến toàn bộ cán bộ, công chức, viên chức và người lao động trong đơn vị thực hiện các quy định của Quy chế này.

2. Định kỳ 02 năm hoặc khi có thay đổi Quy chế bảo đảm ATTT thì kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung trước khi công bố áp dụng.

3. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, các đơn vị phản ánh về Trung tâm Điều tra, Quan trắc đa dạng sinh học để tổng hợp, trình Cục trưởng xem xét, sửa đổi, bổ sung Quy chế ./.