BỘ NÔNG NGHIỆP VÀ PHÁT TRIỂN NÔNG THÔN **CỤC LÂM NGHIỆP**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 235 /QĐ-LN-CĐS	*Hà Nội, ngày 10 tháng 10 năm 2023*

QUYẾT ĐỊNH

Ban hành Quy chế đảm bảo an toàn thông tin mạng, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin của các đơn vị thuộc Cục Lâm nghiệp

CỤC TRƯỞNG CỤC LÂM NGHIỆP

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 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 Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ về việc quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ về bảo vệ dữ liệu cá nhân;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ ban hành Quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ trưởng 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 Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Thông tư số 24/2020/TT-BCA ngày 10/3/2020 của Bộ trưởng Bộ Công an Ban hành biểu mẫu sử dụng trong công tác bảo vệ bí mật nhà nước;

Căn cứ Nghị định số 26/2020/NĐ-CP ngày 28/02/2020 của Chính phủ Quy định chi tiết một số điều của Luật Bảo vệ bí mật Nhà nước;

Căn cứ Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

Căn cứ Quyết định số 1589/QĐ-BNN-TCCB ngày 19 tháng 4 năm 202023 của Bộ trưởng Bộ Nông nghiệp và Phát triển nông thôn quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Cục Lâm nghiệp thuộc Bộ Nông nghiệp và Phát triển nông thôn;

Căn cứ Quyết định số 87/QĐ-LN-VP ngày 27 tháng 7 năm 2023 của Cục trưởng Cục Lâm nghiệp ban hành Quy chế tiếp nhận, xử lý, quản lý, lưu trữ văn

bản và bảo vệ bí mật nhà nước của Cục Lâm nghiệp;

Căn cứ Kế hoạch Công tác Văn thư - Lưu trữ, bảo vệ bí mật nhà nước số 620/KH-LN-VP ngày 14/8/2023;

Theo đề nghị của Trưởng phòng Thông tin và Chuyển đổi số và Chánh Văn phòng Cục Lâm nghiệp.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các đơn vị thuộc Cục Lâm nghiệp.

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

Điều 3. Chánh Văn phòng Cục; thủ trưởng các phòng, đơn vị thuộc Cục; toàn thể công chức, viên chức và người lao động Cục Lâm nghiệp chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Thứ trưởng Nguyễn Quốc Trị (để báo cáo);
- Trung tâm CĐS&TKNN;
- Văn phòng Bộ;
- Lãnh đạo Cục;
- Lưu: VT, CĐS.

CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC LÂM NGHIỆP
BỘ NÔNG NGHIỆP VÀ PHÁT TRIỂN NÔNG THÔN

Trần Quang Bảo

BỘ NÔNG NGHIỆP
VÀ PHÁT TRIỂN NÔNG THÔN
CỤC LÂM NGHIỆP

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

QUY CHẾ

Đảm bảo an toàn thông tin mạng, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin của các đơn vị thuộc Cục Lâm nghiệp

(kèm theo Quyết định số /QĐ-LN-CĐS ngày tháng năm 2023 của Cục trưởng Cục Lâm nghiệp)

Chương I

QUI ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Phạm vi áp dụng: Quy chế này quy định về công tác đảm bảo an toàn thông tin điện tử (ATTT) trong hoạt động ứng dụng công nghệ thông tin (CNTT) của các đơn vị thuộc Cục Lâm nghiệp.

2. Quy chế này áp dụng đối với các đơn vị thuộc Cục Lâm nghiệp gồm:

a) Công chức, viên chức và người lao động (sau đây gọi chung là công chức, viên chức) trong các cơ quan, phòng thuộc Cục; các cơ quan, tổ chức, cá nhân có quan hệ làm việc với Cục.

b) Cơ quan, tổ chức, cá nhân có sử dụng hoặc kết nối truy cập vào hệ thống mạng của Cục.

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin, chính phủ điện tử, chính phủ số và an toàn thông tin cho các đơn vị trực thuộc Cục.

Điều 2. Giải thích từ ngữ

1. An toàn thông tin mạng là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

2. An ninh mạng là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

3. Mạng là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

4. Hệ thống thông tin là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng.

5. Hạ tầng kỹ thuật là tập hợp các thiết bị tính toán, lưu trữ, thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, đường truyền, mạng nội bộ, mạng diện rộng;

6. Trang thiết bị công nghệ thông tin là một nhóm hay một dòng sản phẩm cố định có khả năng xử lý dữ liệu và truyền tải thông tin dữ liệu qua lại giữa những người sử dụng.

7. Thiết bị xử lý thông tin là thiết bị dùng để tạo lập, xử lý, lưu trữ, truyền đưa thông tin dưới dạng điện tử (máy tính, máy in, điện thoại thông minh, thiết bị mạng, thiết bị an ninh mạng, camera giám sát và các thiết bị tương đương khác).

8. Người dùng là cán bộ, công chức, viên chức, người lao động tại các cơ quan, đơn vị thuộc Bộ sử dụng máy tính để xử lý công việc.

9. Phần mềm độc hại là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

10. Trang thông tin điện tử tích hợp các kênh thông tin, các dịch vụ và ứng dụng theo một phương thức thống nhất, thông qua một điểm truy cập duy nhất đối với người sử dụng (từ nay gọi chung là website).

11. Cổng giao tiếp (Port) dùng để định danh các ứng dụng gửi và nhận dữ liệu, mỗi ứng dụng sẽ tương ứng với một cổng giao tiếp, những ứng dụng phổ biến được đặt với số hiệu cổng định trước, nhằm định danh duy nhất các ứng dụng đó. Khi máy tính sử dụng dịch vụ nào thì cổng giao tiếp tương ứng với dịch vụ đó sẽ mở.

12. Bản ghi nhật ký hệ thống (Logfile) là một tập tin được tạo ra trên mỗi thiết bị của hệ thống thông tin như: Tường lửa, máy chủ ứng dụng,... có chứa tất cả thông tin về các hoạt động xảy ra trên thiết bị đó. Bản ghi nhật ký hệ thống dùng để phân tích những sự kiện đã xảy ra, nguồn gốc và các kết quả để có các biện pháp xử lý thích hợp.

Điều 3. Phạm vi và tài nguyên đảm bảo an toàn thông tin

1. Hệ thống mạng của Cục Lâm nghiệp, bao gồm:

- Hệ thống đường truyền dữ liệu, đường kết nối Internet;

- Hệ thống mạng có dây, không dây;

- Các trang thiết bị CNTT được kết nối mạng trong đơn vị.

2. Hệ thống tài nguyên mạng và ứng dụng CNTT, bao gồm:

- Hệ thống thư điện tử;

- Hệ thống thông tin quản lý và cơ sở dữ liệu chuyên ngành;

- Trang thông tin điện tử và hệ thống các website;

- Các phần mềm ứng dụng phục vụ công tác quản lý, điều hành hoạt động của cơ quan nhà nước.

3. Hệ thống máy chủ Cục Lâm nghiệp

Điều 4. Nguyên tắc bảo đảm an toàn, an ninh thông tin mạng

1. Bảo đảm an toàn, an ninh thông tin mạng là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình liên quan đến thông tin, đồng bộ từ khi thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ hệ thống thông tin (dừng hoạt động). Bảo đảm an toàn, an ninh thông tin mạng phải tuân thủ các nguyên tắc chung, được quy định tại Điều 4 Luận An ninh mạng, Điều 4 Luật An toàn thông tin mạng và Điều 4 Nghị định số 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ.

2. Phân cấp, ủy quyền trách nhiệm bảo đảm an toàn an ninh mạng phù hợp với tổ chức bộ máy và phương thức làm việc của Bộ.

3. An toàn thông tin mạng phải gắn liền và hỗ trợ các hoạt động ứng dụng công nghệ thông tin, chính phủ điện tử, chính phủ số, chuyển đổi số của Cục; hỗ trợ việc sử dụng trang thiết bị công nghệ thông tin, thiết bị xử lý thông tin để xử lý công việc của người dùng.

4. Ứng cứu sự cố an toàn thông tin mạng là hoạt động quan trọng nhằm phát hiện, ngăn chặn, xử lý và khắc phục kịp thời sự cố an toàn an ninh mạng.

5. Người dùng nêu cao tinh thần chủ động, tự giác trong việc áp dụng các biện pháp bảo đảm an toàn an ninh mạng.

Điều 5. Các hành vi bị nghiêm cấm

1. Tấn công, vô hiệu hóa trái phép làm mất tác dụng của biện pháp bảo vệ ATTT cho hệ thống thông tin; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để cố ý vượt qua biện pháp kiểm soát truy cập, tấn công, chiếm quyền điều khiển trái phép đối với hệ thống thông tin.

2. Phát tán thư rác, tin nhắn rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.

3. Làm thay đổi hệ thống mạng: tự ý lắp đặt thêm bộ chuyển mạch (swich), lắp đặt thêm mạng không dây, cấu hình địa chỉ IP,...

4. Cấm lưu trữ, đưa lên mạng hoặc trao đổi các thông tin sau:

a) Thông tin chưa được cấp có thẩm quyền công bố.

b) Thông tin thuộc danh mục thông tin mật do pháp luật hiện hành quy định.

c) Thông tin và các dịch vụ thông tin trái với quy định của pháp luật hiện hành như:

- Gây ảnh hưởng đến an ninh quốc gia;

- Xuyên tạc, tuyên truyền chống đối chính sách và pháp luật của Nhà nước;

- Có nội dung kích động bạo lực, tuyên truyền chiến tranh xâm lược, gây hận thù giữa các dân tộc và nhân dân các nước, truyền bá tư tưởng phản động;

- Có ảnh hưởng đến văn hoá xã hội và thuần phong mỹ tục;

- Giả mạo nguồn gốc của thông tin;

- Có ảnh hưởng xấu đến đời tư người khác: quấy rối cá nhân, xúc phạm danh dự, vu khống, xúc phạm đến nhân phẩm người khác.

Chương II

NỘI DUNG, BIỆN PHÁP BẢO ĐẢM AN TOÀN THÔNG TIN

Điều 6. Lưu trữ và trao đổi thông tin

1. Việc lưu trữ và trao đổi thông tin phải tuân thủ các quy định của pháp luật về lưu trữ, CNTT và truyền thông.

2. Các dữ liệu, thông tin và tài liệu quan trọng, ở các mức độ mật, tối mật, tuyệt mật thì người sử dụng phải soạn thảo, lưu trữ tại máy tính soạn thảo văn bản bí mật nhà nước do Cục Lâm nghiệp bố trí máy tính không kết nối mạng. Phải đặt mật khẩu, mã hóa dữ liệu và các biện pháp đảm bảo an toàn, an ninh thông tin, tuân thủ tuyệt đối nội quy Bảo vệ bí mật nhà nước và ANM được đặt tại phòng soạn thảo BMNN.

Điều 7. Yêu cầu về công tác bảo đảm an toàn thông tin

1. Đơn vị quản trị Công nghệ thông tin quản trị hệ thống mạng nội bộ của cơ quan Cục và hệ thống phải được trang bị hệ thống kỹ thuật, công nghệ hiện đại; thường xuyên được quản lý, giám sát, kiểm soát nhằm phát hiện và ngăn chặn các truy cập trái phép của người sử dụng và tin tặc.

2. Xây dựng hệ thống dự phòng cho các hệ thống CNTT cốt lõi như: máy chủ web, cơ sở dữ liệu, thư điện tử. Phải có quy trình phục hồi, sao lưu dữ liệu định kỳ cho hệ thống các phần mềm và cơ sở dữ liệu.

3. Quản lý chặt chẽ hệ thống tài khoản người sử dụng của các hệ thống thông tin, thư điện tử, và các tài nguyên mạng khác gồm các công việc: tạo mới, kích hoạt, sửa đổi, vô hiệu hoá, xoá bỏ,... Phải có biện pháp khóa hoặc hủy tài khoản, quyền truy nhập, thu hồi các thiết bị liên quan tới hệ thống thông tin (khóa, thẻ nhận dạng,...) cho phù hợp đối với công chức, viên chức đã nghỉ việc hoặc chuyển công tác.

4. Hệ thống thông tin quản lý, hệ thống cơ sở dữ liệu, hệ thống máy chủ phải có chức năng tự động ghi nhật ký (trong khoảng thời gian nhất định, tối thiểu là 3 tháng) quá trình đăng nhập vào hệ thống, các thao tác cấu hình hệ thống và các thông tin liên quan về ATTT để phục vụ công tác khắc phục sự cố và điều tra về ATTT khi xảy ra.

5. Việc tiêu huỷ thiết bị hoặc vật mang thông tin (đĩa cứng, đĩa di động,...) phải đảm bảo yêu cầu không để lộ, lọt thông tin nhà nước. Phải có quy trình cụ thể và phải lưu giữ hồ sơ, biên bản, tiêu huỷ.

Điều 8. Một số biện pháp quản lý vận hành đảm bảo an toàn thông tin

1. Đơn vị sử dụng hệ thống

a) Bố trí công chức, viên chức tham gia phối hợp triển khai ATTT.

b) Máy tính bố trí cho các công chức, viên chức thực hiện nhiệm vụ được cài đặt ứng dụng văn phòng và phần mềm diệt virus bản quyền. Người dùng sử dụng có trách nhiệm bảo quản, nghiêm cấm gỡ cài đặt các ứng dụng văn phòng và diệt virus đã được cài đặt. Thông tin cho bộ phận quản trị CNTT khi bản quyền hết hạn để cập nhật thông tin bản quyền kịp thời.

c) Người dùng phải đặt mật khẩu cho máy tính (mật khẩu đăng nhập, mật khẩu bảo vệ màn hình). Sử dụng các thiết bị lưu trữ thông tin (USB, ổ cứng gắn ngoài, thẻ nhớ,...) đảm bảo an toàn, đúng cách để phòng ngừa vi rút, phần mềm gián điệp xâm nhập máy tính phá hoại, đánh cắp thông tin. Định kỳ thường xuyên quét vi rút, phần mềm gián điệp trên máy tính.

2. Phòng Thông tin và Chuyển đổi số:

a) Tham mưu cho lãnh đạo Cục triển khai thực hiện các biện pháp để đảm bảo an toàn, an ninh hệ thống thông tin của cơ quan, đơn vị. Thường xuyên nghiên cứu, cập nhật các kiến thức về ATTT, có biện pháp phòng tránh các nguy cơ tiềm ẩn có thể gây mất thông tin khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ.

b) Thường xuyên cập nhật cấu hình chuẩn cho các thành phần của hệ thống thông tin, thiết lập cấu hình chặt chẽ nhất nhưng vẫn đảm bảo duy trì hoạt động thường xuyên của hệ thống thông tin.

c) Khi thiết lập cấu hình hệ thống thông tin cần xác định các chức năng, cổng giao tiếp mạng, giao thức và dịch vụ không cần thiết để cấm hoặc hạn chế sử dụng.

d) Thường xuyên thực hiện việc theo dõi bản ghi nhật ký hệ thống và các sự kiện khác có liên quan để đánh giá, báo cáo mức độ nghiêm trọng các rủi ro đó. Các rủi ro đó có thể xảy ra do sự truy cập trái phép, sử dụng trái phép, mất, thay đổi hoặc phá hủy thông tin và hệ thống thông tin.

đ) Kiểm soát chặt chẽ việc cài đặt phần mềm vào máy trạm và máy chủ.

Điều 9. Một số biện pháp quản lý kỹ thuật đảm bảo an toàn thông tin

1. Tổ chức mô hình mạng:

Khuyến khích cài đặt, cấu hình, tổ chức hệ thống mạng theo mô hình máy trạm/máy chủ (Clients/Server), hạn chế sử dụng mô hình mạng ngang hàng. Các đơn vị có nhiều phòng, ban, đơn vị trực thuộc không nằm trong cùng một khu

vực, cần thiết lập mạng riêng ảo (Virtual Private Network - VPN) để đảm bảo an ninh cho mạng nội bộ. Khi thiết lập các dịch vụ trên môi trường mạng Internet, chỉ cung cấp những chức năng thiết yếu nhất bảo đảm duy trì hoạt động của hệ thống thông tin; hạn chế sử dụng chức năng, cổng giao tiếp mạng, giao thức và các dịch vụ không cần thiết.

2. Quản lý hệ thống mạng không dây:

Khi thiết lập mạng không dây để kết nối với mạng cục bộ thông qua các điểm truy nhập, cần thiết lập các tham số như: Tên, nhận dạng dịch vụ (Service set identification - SSID), mật khẩu, cấp phép truy cập đối với địa chỉ vật lý (MAC address), mã hóa dữ liệu và thông báo các thông tin liên quan đến điểm truy nhập để cơ quan sử dụng, thường xuyên thay đổi mật khẩu nhằm tăng cường công tác bảo mật.

3. Quản lý đăng nhập hệ thống:

a) Các hệ thống thông tin cần giới hạn lần đăng nhập sai liên tiếp. Nếu liên tục đăng nhập sai vượt quá số lần quy định, hệ thống phải tự động khóa tài khoản hoặc cô lập tài khoản trong một khoảng thời gian nhất định trước khi tiếp tục cho đăng nhập. Tăng cường áp dụng biện pháp bảo mật hai lớp (2-step verification) đối với những ứng dụng quan trọng về bảo mật thông tin.

b) Tổ chức theo dõi, kiểm soát tất cả các phương pháp truy nhập từ xa (quay số, Internet,...) tới hệ thống thông tin, bao gồm cả sự truy nhập có chức năng quản trị, tăng cường sử dụng mạng riêng ảo khi có nhu cầu làm việc từ xa; có biện pháp khoá, chặn quyền truy nhập tới hệ thống đối với những tài khoản có dấu hiệu hoặc bị rò rỉ thông tin truy cập.

c) Yêu cầu người dùng đặt mật khẩu với độ an toàn cao (có chữ thường, có chữ in hoa, có số và ký tự đặc biệt như @, #, !,...) và thường xuyên thay đổi mật khẩu 03 lần/tháng.

4. Chống mã độc, vi rút:

Lựa chọn, triển khai các phần mềm chống vi rút, thư rác có hiệu quả trên các máy chủ, máy trạm, các thiết bị, phương tiện kỹ thuật trong mạng, các hệ thống thông tin quan trọng như: Cổng/Trang thông tin điện tử, thư điện tử, một cửa điện tử,..; đồng thời, thường xuyên cập nhật phiên bản mới, bản vá lỗi của các phần mềm chống vi rút, nhằm kịp thời phát hiện, loại trừ mã độc máy tính (vi rút, trojan, worms,..).

5. Tổ chức quản lý tài nguyên:

Kiểm tra, giám sát chức năng chia sẻ thông tin. Tổ chức cấp phát tài nguyên trên máy chủ theo danh mục thư mục cho từng phòng/ban; khuyến cáo người sử

dụng cân nhắc việc chia sẻ tài nguyên cục bộ trên máy đang sử dụng, khi thực hiện việc chia sẻ tài nguyên cần phải sử dụng mật khẩu để bảo vệ thông tin.

6. Các biện pháp kỹ thuật bảo đảm an toàn cho website:

a) Xác định cấu trúc thiết kế website: Quản lý toàn bộ các phiên bản của mã nguồn, phối hợp với đơn vị thực hiện dịch vụ thuê máy chủ (hosting) tổ chức mô hình trang web hợp lý tránh khả năng tấn công leo thang đặc quyền. Yêu cầu đơn vị cung cấp dịch vụ hosting phải cài đặt các hệ thống phòng vệ như tường lửa (firewall), thiết bị phát hiện/phòng chống xâm nhập (IDS/IPS) ở mức ứng dụng web (WAF - Web Application Firewall).

b) Vận hành ứng dụng website an toàn: Các website khi đưa vào sử dụng hoặc khi bổ sung thêm các chức năng, dịch vụ công mới cần đánh giá kiểm định nhằm tránh được các lỗi bảo mật thường xảy ra trên ứng dụng web như: SQL Injection, Cross-Site Scripting (xss), Broken Authentication and Session Management, Insecure Direct Object References, Cross Site Request Forgery (CSRF), Security Misconfiguration, Failure to Restrict URL Access, Insecure Cryptographic Storage, Insufficient Transport Layer Protection, Unvalidated Redirects and Forwards và các lỗi khác.

c) Thiết lập và cấu hình cơ sở dữ liệu an toàn:

- Luôn cập nhật bản vá lỗi mới nhất cho hệ quản trị cơ sở dữ liệu; sử dụng công cụ để đánh giá, tìm kiếm lỗ hổng trên máy chủ cơ sở dữ liệu;

- Gỡ bỏ các cơ sở dữ liệu không sử dụng;

- Có cơ chế sao lưu dữ liệu, tài liệu hóa quá trình thay đổi cấu trúc bằng cách xây dựng nhật ký cơ sở dữ liệu với các nội dung như: Nội dung thay đổi, lý do thay đổi, thời gian, vị trí thay đổi.

d) Phối hợp với các nhà cung cấp dịch vụ hosting xây dựng phương án phục hồi website, trong đó chú ý ít nhất mỗi tháng thực hiện việc sao lưu toàn bộ nội dung trang web 01 lần bao gồm mã nguồn, cơ sở dữ liệu, dữ liệu phi cấu trúc để bảo đảm khi có sự cố có thể khắc phục trong thời gian ngắn nhất.

7. Thiết lập cơ chế sao lưu và phục hồi hệ thống:

Hệ thống thông tin phải có cơ chế sao lưu thông tin ở mức người dùng và mức hệ thống, được lưu trữ tại nơi an toàn; đồng thời, thường xuyên kiểm tra để đảm bảo tính sẵn sàng phục hồi và toàn vẹn thông tin. Cần có biện pháp sao lưu dự phòng thông tin dữ liệu tại địa chỉ ngoài Bộ phòng ngừa trường hợp bất khả kháng (thiên tai, lũ lụt, động đất, hỏa hoạn, …).

8. Xử lý khẩn cấp:

Khi phát hiện hệ thống máy chủ bị tấn công, thông qua các dấu hiệu như luồng tin tăng lên bất ngờ, nội dung trang chủ bị thay đổi, hệ thống hoạt động rất chậm khác thường,... cần thực hiện các bước cơ bản sau:

a) Bước 1: Ngắt kết nối máy chủ ra khỏi mạng.

b) Bước 2: Sao chép logfile và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ (phục vụ cho công tác phân tích).

c) Bước 3: Khôi phục hệ thống bằng cách chuyển dữ liệu dự phòng (backup) mới nhất để hệ thống hoạt động.

d) Bước 4: Thông báo cho cơ quan chức năng để được hướng dẫn, hỗ trợ.

9. Hệ thống thông tin tại các đơn vị cần có cơ chế ngăn chặn hoặc hạn chế các sự cố gây ra do tấn công từ chối dịch vụ (DoS, DDoS). Sử dụng các thiết bị đặt tại biên của mạng để lọc các gói tin nhằm bảo vệ các thiết bị bên trong, tránh bị ảnh hưởng trực tiếp bởi tấn công từ chối dịch vụ. Đối với hệ thống thông tin cho phép truy nhập công cộng có thể thực hiện bảo vệ bằng cách tăng dung lượng, băng thông hoặc thiết lập hệ thống dự phòng.

Chương III
TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG VÀ TỔ CHỨC THỰC HIỆN

Điều 10. Trách nhiệm Phòng Thông tin và Chuyển đổi số

1. Tham mưu Cục trưởng về công tác bảo đảm ATTT tại Cục và chịu trách nhiệm trước Cục trưởng trong việc đảm bảo ATTT cho các hệ thống CNTT được giao phụ trách.

2. Hàng năm xây dựng kế hoạch, tổng hợp kinh phí để triển khai công tác ATTT trong hoạt động ứng dụng CNTT của Cục.

3. Phối hợp với các phòng ban thuộc Cục triển khai các nhiệm vụ ATTT.

4. Xây dựng và triển khai các chương trình đào tạo, hội nghị tuyên truyền ATTT trong công tác quản lý nhà nước.

5. Thông báo đến phòng ban biết và có biện pháp phòng ngừa, ngăn chặn các nguy cơ mất ATTT do vi rút, phần mềm gián điệp,... gây ra.

6. Chủ trì, phối hợp với các cơ quan liên quan thành lập đoàn kiểm tra, tiến hành kiểm tra định kỳ hoặc đột xuất khi phát hiện có các dấu hiệu, hành vi vi phạm ATTT.

7. Hàng năm, tổng hợp và báo cáo Cục trưởng tình hình triển khai ATTT.

Điều 11. Trách nhiệm của Văn phòng Cục

1. Mua sắm máy tính cho người dùng, tổng hợp thống kê tài sản Công nghệ thông tin theo quy định. Bố trí trang thiết bị và phòng thực hiện soạn thảo văn bản bí mật nhà nước.

2. Tổ chức thanh lý, chuyển giao tài sản Công nghệ thông tin. Bố trí chuyên viên phối hợp với phòng Thông tin và Chuyển đổi số trong các hoạt động Công nghệ thông tin của Cục

Điều 12. Trách nhiệm của công chức, viên chức

1. Thực hiện các biện pháp bảo đảm an toàn thông tin, an ninh mạng và bảo vệ bí mật nhà nước theo điều 8,9 được quy định tại Quy chế.

2. Phản ánh lại các vấn đề vướng mắc cho Văn phòng và Phòng Thông tin và Chuyển đổi số.

Điều 13. Điều khoản thi hành

Chánh Văn phòng Cục; Trưởng các phòng thuộc Cục, Quỹ bảo vệ phát triển rừng Việt Nam có trách nhiệm phổ biến và tổ chức thực hiện Quy chế này.

Trong quá trình thực hiện, nếu có vướng mắc, phát sinh, các cơ quan, đơn vị kịp thời phản ánh về phòng Thông tin và Chuyển đổi số để tổng hợp, báo cáo Cục trưởng xem xét sửa đổi, bổ sung quy chế cho phù hợp./.

CỤC LÂM NGHIỆP