VIỆN KH LÂM NGHIỆP VIỆT NAM
TRUNG TÂM CHỨNG NHẬN QUẢN LÝ RỪNG BỀN VỮNG

Số: 20 /QĐ-TTQLRBV

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

Hà Nội, ngày 07 tháng 10 năm 2026

QUYẾT ĐỊNH
Về việc Ban hành Quy chế quản lý thông tin và bảo đảm an toàn, an ninh mạng của Trung tâm Chứng nhận Quản lý rừng bền vững

GIÁM ĐỐC TRUNG TÂM CHỨNG NHẬN QUẢN LÝ RỪNG BỀN VỮNG

Căn cứ Luật An ninh mạng ngày 10 tháng 12 năm 2025;

Căn cứ Luật Dữ liệu ngày 30 tháng 11 năm 2024;

Căn cứ Luật Bảo vệ dữ liệu cá nhân ngày 26 tháng 6 năm 2025;

Căn cứ Luật Giao dịch điện tử ngày 22 tháng 6 năm 2023;

Căn cứ Luật Lưu trữ ngày 21 tháng 6 năm 2024;

Căn cứ Luật Bảo vệ bí mật nhà nước ngày 10 tháng 12 năm 2025;

Căn cứ Luật Trí tuệ nhân tạo ngày 10 tháng 12 năm 2025;

Căn cứ Nghị định số 356/2025/NĐ-CP ngày 31 tháng 12 năm 2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân;

Căn cứ Nghị định số 331/2026/NĐ-CP ngày 19 tháng 8 năm 2026 của Chính phủ về bảo vệ an ninh mạng đối với hệ thống thông tin;

Căn cứ Nghị định số 333/2026/NĐ-CP ngày 19 tháng 8 năm 2026 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật An ninh mạng;

Căn cứ Quyết định số 3182/QĐ-BNNMT ngày 11/8/2026 của Bộ trưởng Bộ Nông nghiệp và Môi trường quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu của Trung tâm Chứng nhận Quản lý rừng bền vững;

Căn cứ Quyết định số 336/QĐ-KHLN ngày 28/09/2026 của Giám đốc Viện Khoa học Lâm nghiệp Việt Nam quy định Điều lệ Tổ chức và Hoạt động của Trung tâm Chứng nhận Quản lý rừng bền vững.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế quản lý thông tin và đảm bảo an toàn, an ninh mạng của Trung tâm Chứng nhận Quản lý rừng bền vững.

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

Điều 3. Trưởng các đơn vị thuộc Trung tâm: Phòng Tổng hợp, Phòng Kỹ thuật, Văn phòng chứng chỉ rừng tại miền Nam; viên chức và người lao động căn cứ Quyết định thi hành./.

Nơi nhận:
- Như Điều 3;
- Viện KHLN VN (báo cáo);
- Lưu: VT.

GIÁM ĐỐC

BỘ NÔNG NGHIỆP VÀ MÔI TRƯỜNG
TRUNG TÂM CHỨNG NHẬN QUẢN LÝ RỪNG BỀN VỮNG
VIỆN KHOA HỌC LÂM NGHIỆP VIỆT NAM

Vũ Tấn Phương

VIỆN KH LÂM NGHIỆP VIỆT NAM
TRUNG TÂM CHỨNG NHẬN QUẢN LÝ RỪNG BỀN VỮNG

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

QUY CHẾ
Quản lý thông tin và bảo đảm an toàn, an ninh mạng của Trung tâm Chứng nhận Quản lý rừng bền vững

(Kèm theo Quyết định số 20/QĐ-TTQLRBV ngày 07 tháng 10 năm 2026 của Giám đốc Trung tâm Chứng nhận Quản lý rừng bền vững)

Chương I
QUY ĐỊNH CHUNG

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

1. Quy chế này quy định việc tạo lập, tiếp nhận, quản lý, cập nhật, lưu trữ, khai thác, sử dụng, chia sẻ và công bố thông tin, dữ liệu; quản lý tài khoản, thiết bị, hệ thống thông tin và cơ sở dữ liệu; bảo đảm an toàn, an ninh mạng; bảo vệ dữ liệu cá nhân; sử dụng công nghệ số và trí tuệ nhân tạo; quản lý nhà cung cấp dịch vụ công nghệ thông tin (CNTT); xử lý sự cố và trách nhiệm của các tổ chức, cá nhân thuộc Trung tâm Chứng nhận Quản lý rừng bền vững (sau đây gọi là Trung tâm).

2. Quy chế này áp dụng đối với:

a) Các phòng, Văn phòng Chứng chỉ rừng tại miền Nam thuộc Trung tâm;

b) Viên chức, người lao động và các cá nhân làm việc, cộng tác hoặc được Trung tâm giao nhiệm vụ có liên quan đến thông tin, dữ liệu và hệ thống thông tin của Trung tâm;

c) Tổ chức, cá nhân cung cấp dịch vụ CNTT, an toàn thông tin, phát triển phần mềm, quản trị hệ thống hoặc có kết nối, truy cập vào hệ thống thông tin, cơ sở dữ liệu và tài nguyên số của Trung tâm.

3. Các nội dung chuyên ngành về chứng nhận, quản lý hồ sơ, tài chính - kế toán, văn thư, lưu trữ, bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân và các lĩnh vực khác được thực hiện theo quy định pháp luật và quy định chuyên ngành có liên quan.

Điều 2. Giải thích từ ngữ

Trong Quy chế này, các từ ngữ dưới đây được hiểu như sau:

1. *Thông tin, dữ liệu* là thông tin, dữ liệu được tạo lập, tiếp nhận, quản lý, lưu trữ hoặc khai thác trong quá trình thực hiện chức năng, nhiệm vụ của Trung tâm, bao gồm dữ liệu chuyên môn, dữ liệu chứng nhận, dữ liệu hành chính, thư điện tử, thông tin lưu giữ trên văn phòng điện tử, các nền tảng số của Trung tâm ; các báo cáo, ấn phẩm và các thông tin khác.

2. *Hệ thống thông tin* là tập hợp phần cứng, phần mềm và 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 không gian mạng.

3. *Cơ sở dữ liệu VFCS* là cơ sở dữ liệu và các hệ thống phục vụ việc quản lý, vận hành, công bố và khai thác thông tin thuộc Hệ thống Chứng chỉ rừng Quốc gia (VFCS) trong phạm vi Trung tâm được giao quản lý.

4. *An ninh mạng* là sự ổn định, an ninh, an toàn của không gian mạng; bảo vệ hệ thống thông tin và bảo đảm thông tin, dữ liệu, 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.

5. *Đầu mối CNTT* là viên chức hoặc người lao động được Giám đốc phân công thực hiện nhiệm vụ tham mưu, quản trị và phối hợp xử lý các vấn đề về CNTT, an toàn, an ninh mạng của Trung tâm.

6. *Người sử dụng* là cá nhân được cấp quyền truy cập hoặc được phép sử dụng hệ thống thông tin, dữ liệu và tài nguyên số của Trung tâm.

Điều 3. Nguyên tắc chung

1. Thông tin, dữ liệu phải được quản lý theo đúng chức năng, nhiệm vụ, thẩm quyền, mục đích sử dụng và quy định của pháp luật.

2. Bảo đảm an toàn, an ninh mạng là trách nhiệm của Trung tâm và của mọi tổ chức, cá nhân sử dụng hoặc quản lý hệ thống thông tin, dữ liệu của Trung tâm.

3. Việc bảo vệ thông tin, dữ liệu phải được thực hiện trong toàn bộ vòng đời: tạo lập, tiếp nhận, xử lý, sử dụng, chia sẻ, công bố, lưu trữ và hủy bỏ.

4. Việc phân quyền truy cập phải theo nguyên tắc đúng người, đúng chức năng, đúng phạm vi và đúng thời gian cần thiết.

5. Dữ liệu phải bảo đảm tính chính xác, đầy đủ, nhất quán, toàn vẹn, khả dụng và có khả năng truy xuất nguồn gốc trong phạm vi phù hợp.

6. Thông tin, dữ liệu phải có đơn vị hoặc cá nhân chịu trách nhiệm quản lý; bảo đảm khả năng truy xuất nguồn gốc, lịch sử cập nhật và trách nhiệm giải trình trong quá trình khai thác, sử dụng.

7. Việc ứng dụng công nghệ số và trí tuệ nhân tạo phải bảo đảm an toàn, bảo mật, tuân thủ pháp luật và có sự kiểm tra của con người đối với các kết quả được sử dụng chính thức.

Điều 4. Các hành vi bị nghiêm cấm

Ngoài các hành vi bị nghiêm cấm theo quy định của pháp luật, tổ chức, cá nhân thuộc phạm vi áp dụng của Quy chế này không được thực hiện các hành vi sau:

1. Truy cập, sử dụng, khai thác, sao chép, sửa đổi, xóa hoặc cung cấp thông tin, dữ liệu, tài khoản hoặc hệ thống thông tin của Trung tâm khi không được phép hoặc vượt quá phạm vi quyền được cấp.

2. Sử dụng tài khoản, thông tin xác thực, khóa truy cập hoặc quyền quản trị của người khác; cho người khác sử dụng tài khoản của mình, trừ trường hợp được phép theo cơ chế quản trị hệ thống.

3. Tự ý thay đổi cấu hình, cài đặt phần mềm, thiết lập kết nối, thay đổi quyền truy cập hoặc thực hiện các thay đổi kỹ thuật có khả năng ảnh hưởng đến an toàn, an ninh hoặc hoạt động của hệ thống.

4. Tự ý xóa, làm mất, làm sai lệch, che giấu hoặc sửa đổi trái phép dữ liệu, nhật ký hệ thống, hồ sơ điện tử hoặc dấu vết liên quan đến hoạt động của hệ thống.

5. Phát tán mã độc, phần mềm độc hại, thư rác, thông tin giả mạo hoặc thực hiện hành vi gây gián đoạn, cản trở, làm suy giảm hoặc phá hoại hoạt động của hệ thống thông tin.

6. Tự ý dò quét, kiểm thử xâm nhập, khai thác lỗ hổng, vượt qua cơ chế kiểm soát truy cập hoặc thực hiện các hành vi nhằm chiếm quyền điều khiển hệ thống khi chưa được Trung tâm cho phép.

7. Tự ý đưa thông tin, dữ liệu của Trung tâm, đặc biệt là dữ liệu cá nhân, dữ liệu hạn chế truy cập, hồ sơ chứng nhận chưa công bố, thông tin xác thực, khóa truy cập hoặc thông tin cần bảo vệ lên các nền tảng, dịch vụ trực tuyến hoặc hệ thống trí tuệ nhân tạo bên ngoài khi chưa được phép.

8. Cung cấp, chia sẻ hoặc công bố thông tin, dữ liệu của Trung tâm ra bên ngoài không đúng thẩm quyền, không đúng mục đích hoặc không phù hợp với phạm vi được phép công khai.

9. Tự ý sao lưu, chuyển dữ liệu của Trung tâm sang thiết bị cá nhân, dịch vụ lưu trữ cá nhân hoặc hệ thống bên ngoài không được Trung tâm cho phép.

10. Che giấu, trì hoãn hoặc không thông báo sự cố, nguy cơ mất an toàn, mất dữ liệu, lộ thông tin hoặc hành vi vi phạm Quy chế mà mình phát hiện.

11. Lợi dụng quyền truy cập, quyền quản trị hoặc vị trí công tác để thu thập, sử dụng hoặc tiết lộ thông tin, dữ liệu trái quy định.

12. Thực hiện các hành vi khác vi phạm pháp luật về an ninh mạng, bảo vệ dữ liệu cá nhân, bảo vệ bí mật nhà nước, dữ liệu và các quy định pháp luật có liên quan.

Chương II
QUẢN LÝ THÔNG TIN VÀ DỮ LIỆU

Điều 5. Phân loại thông tin, dữ liệu

1. Thông tin, dữ liệu của Trung tâm được phân loại phục vụ công tác quản lý, khai thác và bảo vệ, phù hợp với quy định pháp luật và yêu cầu quản lý nội bộ, gồm:

a) Thông tin, dữ liệu được công khai;

b) Thông tin, dữ liệu nội bộ;

c) Thông tin, dữ liệu hạn chế truy cập;

d) Dữ liệu cá nhân;

đ) Thông tin thuộc bí mật nhà nước ;

e) Thông tin phải bảo vệ theo quy định pháp luật hoặc cam kết bảo mật.

2. Việc công khai, cung cấp, chia sẻ và khai thác từng loại thông tin, dữ liệu phải thực hiện theo thẩm quyền và quy định pháp luật có liên quan.

3. Phòng Tổng hợp chủ trì tham mưu nguyên tắc phân loại đối với thông tin, dữ liệu dùng chung; các phòng chịu trách nhiệm phân loại dữ liệu chuyên môn thuộc phạm vi quản lý.

Điều 6. Tạo lập, tiếp nhận, cập nhật và quản lý dữ liệu

1. Đơn vị, cá nhân tạo lập hoặc cung cấp dữ liệu chịu trách nhiệm về tính chính xác, đầy đủ, hợp pháp và kịp thời của dữ liệu trong phạm vi trách nhiệm được giao.

2. Đơn vị chủ trì nhiệm vụ chịu trách nhiệm quản lý, cập nhật, bảo đảm tính chính xác, đầy đủ, kịp thời và bảo mật đối với dữ liệu phát sinh trong quá trình thực hiện nhiệm vụ được giao.

3. Dữ liệu trước khi đưa vào hệ thống phải được kiểm tra, xử lý và cập nhật theo quy trình chuyên môn tương ứng.

4. Việc sửa đổi dữ liệu phải được thực hiện bởi người có thẩm quyền; đối với dữ liệu chứng nhận và dữ liệu đã công bố, việc sửa đổi phải bảo đảm khả năng truy xuất lịch sử thay đổi theo khả năng kỹ thuật của hệ thống.

5. Không được tự ý xóa, sửa, sao chép hoặc làm thay đổi dữ liệu ngoài phạm vi được giao.

Điều 7. Khai thác, sử dụng, cung cấp và công bố thông tin

1. Người sử dụng chỉ được khai thác và sử dụng thông tin, dữ liệu phù hợp với chức năng, nhiệm vụ và quyền truy cập được cấp.

2. Việc cung cấp, chia sẻ hoặc công bố thông tin, dữ liệu ra bên ngoài Trung tâm phải đúng thẩm quyền, mục đích, phạm vi được phép và tuân thủ quy định pháp luật, trừ trường hợp pháp luật có quy định khác.

3. Thông tin công bố trên website, cơ sở dữ liệu công khai và các nền tảng số của Trung tâm phải được kiểm tra về nội dung, thẩm quyền công bố và phạm vi thông tin được phép công khai.

4. Không được cung cấp dữ liệu cá nhân, dữ liệu hạn chế truy cập hoặc thông tin cần bảo vệ cho bên thứ ba khi chưa có căn cứ và thẩm quyền phù hợp.

Điều 8. Lưu trữ, sao lưu và hủy thông tin, dữ liệu

1. Thông tin, dữ liệu phải được lưu trữ phù hợp với giá trị, mục đích sử dụng và thời hạn lưu trữ theo quy định pháp luật và quy định của Trung tâm.

2. Dữ liệu quan trọng của Trung tâm phải được sao lưu theo phương án phù hợp với yêu cầu về an toàn và khả năng khôi phục của hệ thống.

3. Việc hủy dữ liệu được thực hiện đúng thẩm quyền, đúng thời hạn và phương thức theo quy định pháp luật, quy định về lưu trữ và quy định của Trung tâm; trường hợp pháp luật yêu cầu tiếp tục lưu giữ thì không thực hiện hủy.

Chương III
QUẢN LÝ CƠ SỞ DỮ LIỆU VÀ HỆ THỐNG THÔNG TIN PHỤC VỤ VFCS

Điều 9. Quản lý cơ sở dữ liệu và hệ thống thông tin VFCS

1. Trung tâm quản lý, vận hành và khai thác cơ sở dữ liệu, hệ thống thông tin phục vụ VFCS trong phạm vi chức năng, nhiệm vụ và thẩm quyền được giao.

2. Phòng Tổng hợp là đầu mối quản lý cơ sở dữ liệu chứng nhận VFCS/PEFC về mặt nghiệp vụ; phối hợp với các phòng, đơn vị và đầu mối CNTT trong việc cập nhật, khai thác và bảo đảm an toàn dữ liệu.

3. Đầu mối CNTT thực hiện quản lý, vận hành kỹ thuật và phối hợp bảo đảm an toàn, an ninh đối với cơ sở dữ liệu và hệ thống thông tin VFCS/PEFC theo phân công.

4. Việc quản lý, vận hành cơ sở dữ liệu và hệ thống thông tin VFCS/PEFC phải bảo đảm tính chính xác, nhất quán, toàn vẹn, khả dụng và khả năng truy xuất lịch sử thay đổi phù hợp với khả năng kỹ thuật.

5. Các thay đổi có ảnh hưởng đến cấu trúc dữ liệu, chức năng chính, quyền quản trị hoặc an toàn của hệ thống phải được xem xét, phê duyệt và ghi nhận theo thẩm quyền.

Điều 10. Quản lý dữ liệu chứng nhận và công bố thông tin

1. Dữ liệu chứng nhận VFCS/PEFC bao gồm thông tin về tổ chức được chứng nhận, chủ rừng, chứng chỉ, phạm vi chứng nhận, tình trạng hiệu lực, giấy phép sử dụng nhãn và các thông tin liên quan theo phạm vi quản lý của Trung tâm.

2. Phòng Tổng hợp có trách nhiệm tổ chức tiếp nhận, kiểm tra, cập nhật và quản lý dữ liệu chứng nhận VFCS/PEFC trên cơ sở hồ sơ, quyết định và thông tin do các phòng, đơn vị có liên quan cung cấp theo chức năng, nhiệm vụ được phân công.

3. Phòng Kỹ thuật và các đơn vị có liên quan có trách nhiệm cung cấp, kiểm tra và phối hợp cập nhật các thông tin, dữ liệu chuyên môn thuộc phạm vi được phân công; chịu trách nhiệm về tính chính xác của nội dung chuyên môn do mình cung cấp.

4. Việc điều chỉnh, đình chỉ, thu hồi hoặc cập nhật trạng thái thông tin chứng nhận được thực hiện trên cơ sở hồ sơ, quyết định hoặc thông tin có thẩm quyền và phải bảo đảm tính chính xác, thống nhất, cập nhật của dữ liệu.

5. Thông tin chứng nhận được công bố trên website, cơ sở dữ liệu công khai hoặc các kênh thông tin khác của Trung tâm theo phạm vi, nội dung và thẩm quyền được xác định; việc công bố phải bảo đảm không làm lộ thông tin thuộc phạm vi hạn chế, dữ liệu cá nhân hoặc thông tin cần bảo vệ theo quy định của pháp luật.

Điều 11. Quản lý dữ liệu trong các hoạt động chuyên môn khác

1. Các phòng chịu trách nhiệm quản lý dữ liệu phát sinh từ hoạt động chuyên môn thuộc phạm vi được giao.

2. Hồ sơ, dữ liệu phục vụ nghiên cứu khoa học, tư vấn, đào tạo, hợp tác quốc tế, đánh giá, chứng nhận, carbon, dịch vụ hệ sinh thái và các hoạt động khác phải được quản lý phù hợp với mục đích sử dụng và yêu cầu bảo mật.

3. Việc chia sẻ dữ liệu với tổ chức, đối tác trong và ngoài nước phải thực hiện theo thẩm quyền, hợp đồng, thỏa thuận hoặc quy định pháp luật có liên quan.

Chương IV
QUẢN LÝ TÀI KHOẢN, THIẾT BỊ VÀ HỆ THỐNG THÔNG TIN

Điều 12. Quản lý tài khoản và quyền truy cập

1. Mỗi cá nhân sử dụng tài khoản được cấp phải chịu trách nhiệm về việc sử dụng tài khoản đó.

2. Không sử dụng tài khoản của người khác hoặc cho người khác sử dụng tài khoản của mình, trừ trường hợp quản trị hệ thống được thực hiện theo cơ chế được phê duyệt.

3. Quyền truy cập phải được cấp theo chức năng, nhiệm vụ và nhu cầu công việc; được rà soát, điều chỉnh hoặc thu hồi khi có thay đổi về nhiệm vụ, vị trí công tác hoặc chấm dứt làm việc.

Điều 13. Quản lý mật khẩu và thông tin xác thực

1. Người sử dụng phải bảo mật mật khẩu, mã xác thực, khóa truy cập, khóa API và các thông tin xác thực khác.

2. Không lưu trữ hoặc chia sẻ thông tin xác thực tại nơi không được phép hoặc qua phương thức không bảo đảm an toàn.

3. Khi phát hiện hoặc nghi ngờ thông tin xác thực bị lộ, phải thông báo ngay cho đầu mối CNTT để xử lý.

Điều 14. Quản lý máy tính, thiết bị và mạng

1. Máy tính, thiết bị mạng, thiết bị lưu trữ và các thiết bị số do Trung tâm quản lý phải được sử dụng đúng mục đích và bảo đảm an toàn.

2. Không tự ý cài đặt phần mềm không rõ nguồn gốc, phần mềm vi phạm bản quyền hoặc phần mềm có nguy cơ ảnh hưởng đến an toàn hệ thống.

3. Không tự ý kết nối thiết bị không được phép vào hệ thống mạng của Trung tâm.

4. Thiết bị chứa dữ liệu của Trung tâm phải được bảo vệ phù hợp khi đưa ra ngoài trụ sở, sửa chữa, thay thế hoặc thanh lý.

Điều 15. Website, thư điện tử, phần mềm và dịch vụ trực tuyến

1. Website, thư điện tử, phần mềm, nền tảng trực tuyến và các dịch vụ số của Trung tâm phải được quản lý theo thẩm quyền và bảo đảm an toàn trong quá trình sử dụng.

2. Nội dung đưa lên website và các kênh thông tin chính thức phải được kiểm tra và phê duyệt theo quy định của Trung tâm.

3. Không sử dụng tài khoản thư điện tử, phần mềm hoặc dịch vụ trực tuyến của Trung tâm để thực hiện hành vi trái pháp luật hoặc gây ảnh hưởng đến uy tín, an toàn và hoạt động của Trung tâm.

Chương V
BẢO ĐẢM AN TOÀN, AN NINH MẠNG VÀ BẢO VỆ DỮ LIỆU

Điều 16. Các biện pháp bảo đảm an toàn, an ninh mạng

1. Trung tâm thực hiện các biện pháp phù hợp để bảo vệ hệ thống thông tin, bao gồm quản lý truy cập, bảo vệ thiết bị và mạng, cập nhật phần mềm, sao lưu dữ liệu, giám sát, phát hiện và xử lý sự cố.

2. Hệ thống thông tin, dữ liệu được xác định là quan trọng theo yêu cầu quản lý của Trung tâm hoặc theo quy định pháp luật phải được sao lưu và có phương án khôi phục phù hợp...

3. Hệ thống thông tin thuộc đối tượng phải xác định cấp độ theo quy định của pháp luật thì thực hiện phân loại, xác định cấp độ và triển khai phương án bảo đảm an toàn thông tin theo quy định.

4. Các hệ thống quan trọng phải được kiểm tra, đánh giá và giám sát an toàn phù hợp với mức độ quan trọng và rủi ro.

5. Nhật ký hệ thống phải được ghi nhận và lưu trữ phù hợp để phục vụ quản lý, kiểm tra và xử lý sự cố.

Điều 17. Bảo vệ dữ liệu cá nhân và thông tin cần bảo vệ

1. Việc thu thập, lưu trữ, sử dụng, cung cấp, chia sẻ và xử lý dữ liệu cá nhân phải đúng mục đích, phạm vi, thẩm quyền và quy định pháp luật.

2. Chỉ những người có nhiệm vụ và quyền truy cập phù hợp mới được tiếp cận dữ liệu cá nhân hoặc thông tin cần bảo vệ.

3. Khi phát hiện nguy cơ mất, lộ, hủy hoại hoặc sử dụng trái phép dữ liệu cá nhân hoặc thông tin cần bảo vệ, phải kịp thời thông báo và xử lý theo quy định.

4. Việc quản lý thông tin thuộc bí mật nhà nước thực hiện theo pháp luật về bảo vệ bí mật nhà nước và quy định riêng của Trung tâm.

Điều 18. Ứng dụng công nghệ số và trí tuệ nhân tạo

1. Trung tâm khuyến khích ứng dụng công nghệ số và trí tuệ nhân tạo để nâng cao hiệu quả quản lý, nghiên cứu, chứng nhận và cung cấp dịch vụ.

2. Không đưa dữ liệu cá nhân, thông tin hạn chế truy cập, hồ sơ chứng nhận chưa công bố, tài khoản, mật khẩu, khóa truy cập hoặc thông tin cần bảo vệ lên hệ thống trí tuệ nhân tạo bên ngoài khi chưa được phép và chưa có biện pháp bảo vệ phù hợp.

3. Kết quả do trí tuệ nhân tạo tạo ra phải được kiểm tra, xác minh bởi người có trách nhiệm trước khi sử dụng làm căn cứ chính thức trong công việc của Trung tâm.

4. Không sử dụng kết quả do trí tuệ nhân tạo tạo ra làm căn cứ duy nhất để ban hành kết luận chuyên môn, quyết định quản lý hoặc công bố chính thức của Trung tâm. Người sử dụng có trách nhiệm kiểm tra, xác minh và bảo đảm nội dung do hệ thống trí tuệ nhân tạo tạo ra hoặc hỗ trợ tạo ra phù hợp với yêu cầu chuyên môn, quy định pháp luật và mục đích sử dụng trước khi sử dụng trong hoạt động của Trung tâm.

Chương VI
QUẢN LÝ NHÀ CUNG CẤP DỊCH VỤ CNTT

Điều 19. Nguyên tắc thuê và sử dụng dịch vụ

1. Việc thuê, mua hoặc sử dụng dịch vụ CNTT phải bảo đảm yêu cầu về chức năng, an toàn, bảo mật, quyền quản lý, khai thác, sử dụng và bảo vệ dữ liệu của Trung tâm.

2. Hợp đồng, thỏa thuận hoặc hồ sơ yêu cầu dịch vụ phải quy định phù hợp về trách nhiệm bảo mật, quyền truy cập, quản lý dữ liệu, xử lý sự cố, bàn giao và chấm dứt quyền truy cập.

Điều 20. Quyền truy cập của nhà cung cấp

1. Nhà cung cấp chỉ được truy cập hệ thống trong phạm vi, thời gian và mục đích được Trung tâm phê duyệt.

2. Việc truy cập quản trị từ xa phải được kiểm soát và ghi nhận phù hợp với khả năng kỹ thuật.

3. Nhà cung cấp không được tự ý sao chép, chuyển giao, sử dụng hoặc tiết lộ dữ liệu của Trung tâm.

Điều 21. Bàn giao và chấm dứt dịch vụ

Khi kết thúc hoặc chấm dứt hợp đồng, nhà cung cấp phải:

1. Bàn giao đầy đủ dữ liệu, tài liệu, cấu hình, tài khoản quản trị và các thành phần thuộc quyền quản lý của Trung tâm theo hợp đồng;

2. Chấm dứt các quyền truy cập không còn cần thiết;

3. Hoàn trả, chuyển giao hoặc xóa dữ liệu của Trung tâm theo hợp đồng, thỏa thuận và quy định pháp luật; việc xóa dữ liệu không áp dụng đối với dữ liệu phải tiếp tục lưu giữ theo quy định;

4. Tiếp tục thực hiện nghĩa vụ bảo mật đối với thông tin đã tiếp cận trong thời gian cung cấp dịch vụ.

Chương VII
XỬ LÝ SỰ CỐ VÀ KHÔI PHỤC HỆ THỐNG

Điều 22. Phát hiện và thông báo sự cố

1. Sự cố bao gồm mất, lộ, sửa đổi trái phép dữ liệu; tài khoản bị xâm phạm; mã độc; tấn công mạng; hệ thống ngừng hoạt động hoặc các sự kiện khác có nguy cơ ảnh hưởng đến an toàn, an ninh thông tin.

2. Người sử dụng khi phát hiện hoặc nghi ngờ có sự cố phải thông báo ngay cho đầu mối CNTT và người phụ trách đơn vị.

3. Không tự ý che giấu, xóa dấu vết hoặc thực hiện các biện pháp có thể làm mất dữ liệu phục vụ điều tra, xử lý sự cố.

Điều 23. Xử lý và khôi phục sự cố

1. Đầu mối CNTT chủ trì phối hợp với đơn vị liên quan đánh giá, cô lập, xử lý và khôi phục hệ thống theo mức độ sự cố.

2. Đối với sự cố nghiêm trọng, phải báo cáo Giám đốc và thực hiện việc phối hợp với đơn vị chuyên môn, nhà cung cấp hoặc cơ quan có thẩm quyền theo quy định.

3. Việc khôi phục phải ưu tiên bảo vệ dữ liệu, duy trì hoạt động thiết yếu và hạn chế thiệt hại.

Điều 24. Báo cáo và lưu hồ sơ sự cố

Sự cố có ảnh hưởng đến dữ liệu, hệ thống hoặc hoạt động của Trung tâm phải được ghi nhận tối thiểu về thời điểm, nguyên nhân hoặc dấu hiệu ban đầu, phạm vi ảnh hưởng, biện pháp xử lý, kết quả khôi phục và kiến nghị phòng ngừa tái diễn.

Chương VIII
TRÁCH NHIỆM VÀ TỔ CHỨC THỰC HIỆN

Điều 25. Trách nhiệm của Giám đốc

1. Chỉ đạo chung và chịu trách nhiệm về công tác quản lý thông tin, dữ liệu và bảo đảm an toàn, an ninh mạng của Trung tâm theo thẩm quyền.

2. Quyết định hoặc phân cấp việc phê duyệt quyền truy cập, công bố thông tin, xử lý sự cố và các vấn đề quan trọng liên quan đến an toàn, an ninh thông tin.

3. Phân công đầu mối CNTT và chỉ đạo bố trí nguồn lực cần thiết để thực hiện Quy chế.

Điều 26. Trách nhiệm của các phòng, đơn vị

1. Phòng Tổng hợp:

a) Đầu mối quản lý dữ liệu chứng nhận VFCS/PEFC theo quy định tại Điều 9 và Điều 10 của Quy chế này; tổ chức tiếp nhận, kiểm tra, cập nhật, quản lý và phối hợp công bố dữ liệu chứng nhận theo thẩm quyền;

Đầu mối quản lý thông tin, dữ liệu chứng nhận VFCS/PEFC,

b) Quản lý thông tin, dữ liệu về tổ chức, nhân sự, hành chính, tài chính, tài sản và các thông tin, dữ liệu khác thuộc phạm vi chức năng, nhiệm vụ được giao; chịu trách nhiệm về tính chính xác, đầy đủ, cập nhật và bảo mật của dữ liệu quản lý;

c) Phối hợp với các phòng, đơn vị và đầu mối CNTT trong việc quản lý tài khoản, thiết bị, hệ thống thông tin và bảo đảm an toàn, an ninh thông tin, dữ liệu của Trung tâm;

d) Theo dõi, tham mưu việc thực hiện Quy chế này; phối hợp tổ chức hướng dẫn, kiểm tra việc quản lý, sử dụng thông tin, dữ liệu trong Trung tâm.

2. Phòng Kỹ thuật:

a) Quản lý và cung cấp thông tin, dữ liệu chuyên môn thuộc phạm vi chức năng, nhiệm vụ được giao;

b) Kiểm tra, bảo đảm tính chính xác, đầy đủ và cập nhật của nội dung chuyên môn do Phòng cung cấp; phối hợp với Phòng Tổng hợp trong việc cập nhật dữ liệu chứng nhận VFCS/PEFC;

c) Phối hợp với các phòng, đơn vị và đầu mối CNTT trong việc khai thác, sử dụng các hệ thống thông tin, cơ sở dữ liệu phục vụ hoạt động chuyên môn.

3. Văn phòng Chứng chỉ rừng tại miền Nam: quản lý thông tin, hồ sơ và dữ liệu phát sinh trong phạm vi chức năng, nhiệm vụ được giao; chịu trách nhiệm về tính chính xác, đầy đủ, cập nhật, bảo mật và lưu trữ dữ liệu theo quy định.

4. Các phòng, đơn vị có trách nhiệm quản lý, bảo vệ và sử dụng thông tin, dữ liệu thuộc phạm vi được giao; kịp thời phối hợp xử lý sai lệch dữ liệu, nguy cơ mất an toàn hoặc sự cố thông tin, hệ thống thông tin theo quy định của Quy chế này.

Điều 27. Trách nhiệm của đầu mối CNTT

1. Tham mưu cho Giám đốc về quản lý, vận hành và bảo đảm an toàn hệ thống thông tin.

2. Quản lý tài khoản quản trị, phân quyền kỹ thuật, sao lưu, giám sát và phối hợp xử lý sự cố theo phân công.

3. Phối hợp với các phòng trong việc kiểm tra, đánh giá an toàn hệ thống và quản lý nhà cung cấp dịch vụ CNTT.

4. Theo dõi, cập nhật các yêu cầu về an toàn, an ninh mạng và đề xuất biện pháp phù hợp với tình hình thực tế.

5. Thực hiện nhiệm vụ quản lý, vận hành kỹ thuật và phối hợp bảo đảm an toàn, an ninh hệ thống thông tin theo phân công; việc quản lý nội dung, tính chính xác, tính đầy đủ, tính cập nhật và tính hợp pháp của thông tin, dữ liệu thuộc trách nhiệm của các đơn vị theo Điều 26 của Quy chế này.

Điều 28. Trách nhiệm của viên chức và người lao động

1. Tuân thủ Quy chế và các quy định, hướng dẫn về an toàn, an ninh thông tin.

2. Bảo vệ tài khoản, thiết bị và thông tin được giao.

3. Không truy cập, sử dụng, sao chép, sửa đổi hoặc cung cấp thông tin, dữ liệu ngoài phạm vi được phép.

4. Chủ động phát hiện và thông báo các nguy cơ, hành vi hoặc sự cố có thể ảnh hưởng đến an toàn thông tin.

5. Tham gia các hoạt động đào tạo, phổ biến kiến thức về an toàn, an ninh mạng theo yêu cầu của Trung tâm.

Điều 29. Trách nhiệm của tổ chức, cá nhân cung cấp dịch vụ

Tổ chức, cá nhân cung cấp dịch vụ cho Trung tâm có trách nhiệm tuân thủ Quy chế này, hợp đồng và các yêu cầu về bảo mật, bảo vệ dữ liệu, quản lý quyền truy cập, xử lý sự cố và bàn giao dữ liệu của Trung tâm.

Điều 30. Kiểm tra, giám sát

1. Trung tâm tổ chức kiểm tra, giám sát việc thực hiện Quy chế phù hợp với yêu cầu quản lý và mức độ rủi ro.

2. Việc kiểm tra có thể bao gồm kiểm tra quyền truy cập, tài khoản, thiết bị, dữ liệu, nhật ký hệ thống, việc sao lưu, việc thực hiện các yêu cầu bảo mật và việc tuân thủ của nhà cung cấp dịch vụ.

3. Kết quả kiểm tra là căn cứ để khắc phục tồn tại và nâng cao hiệu quả bảo đảm an toàn, an ninh mạng.

Điều 31. Xử lý vi phạm

Tổ chức, cá nhân vi phạm Quy chế, làm mất, lộ, hư hỏng hoặc sử dụng trái phép thông tin, dữ liệu, tài khoản hoặc hệ thống thông tin của Trung tâm, tùy theo tính chất,

mức độ vi phạm, phải chịu trách nhiệm theo quy định của pháp luật, nội quy của Trung tâm và các thỏa thuận có liên quan.

Điều 32. Tổ chức thực hiện

1. Các đơn vị thuộc Trung tâm và toàn thể VC&NLĐ thực hiện nghiêm Quy chế này.

2. Các đơn vị trực thuộc, viên chức và người lao động phụ trách xây dựng quy trình, hướng dẫn kỹ thuật về quản lý tài khoản, sao lưu, xử lý sự cố, quản trị hệ thống, sử dụng thư điện tử, thiết bị, phần mềm và trí tuệ nhân tạo để thực hiện đảm bảo thống nhất trong quản lý thông tin và đảm bảo an toàn, an ninh mạng.

3. Trong quá trình thực hiện, nếu phát sinh vấn đề hoặc quy định pháp luật có thay đổi, Lãnh đạo đơn vị trực thuộc phản ánh về Phòng Tổng hợp để tổng hợp, báo cáo Giám đốc xem xét sửa đổi, bổ sung Quy chế./.