

BỘ TƯ PHÁP

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

Số: 2750/QĐ-BTP

Hà Nội, ngày 04 tháng 9 năm 2025

QUYẾT ĐỊNH

**Ban hành Quy chế Bảo đảm an toàn thông tin,
an ninh mạng cho các hệ thống thông tin, phần mềm ứng dụng
và Nền tảng số trong lĩnh vực thi hành án dân sự**

BỘ TRƯỞNG BỘ TƯ PHÁP

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19 tháng 11 năm 2015;

Căn cứ Luật An ninh mạng số 24/2018/QH14 ngày 12 tháng 6 năm 2018;

Căn cứ Luật Bảo vệ bí mật nhà nước số 29/2018/QH14 ngày 15 tháng 11 năm 2018;

Căn cứ Nghị định số 39/2025/NĐ-CP ngày 26 tháng 02 năm 2025 của Chính phủ quy định về chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Tư pháp;

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 tháng 8 năm 2022 của Chính phủ về Quy định chi tiết một số điều của Luật An ninh mạng;

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 Quyết định số 2692/QĐ-BTP ngày 09 tháng 11 năm 2023 của Bộ trưởng Bộ Tư pháp Ban hành Quy chế Bảo đảm an toàn, an ninh thông tin mạng theo cấp độ cho Trung tâm dữ liệu điện tử Bộ Tư pháp;

Theo đề nghị của Cục trưởng Cục Quản lý Thi hành án dân sự.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế Bảo đảm an toàn thông tin, an ninh mạng cho các các hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực thi hành án dân sự.

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

Điều 3. Cục trưởng Cục Quản lý Thi hành án dân sự, Thủ trưởng các đơn vị thuộc Cục Quản lý Thi hành án dân sự, Trưởng Thi hành án dân sự tỉnh, thành

phổ và cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- Như điều 3;
- Bộ trưởng (để b/c);
- Cục CNTT (để th/h);
- Cục Quản lý THADS (để th/h);
- Thủ trưởng các đơn vị thuộc Cục QLTHADS (để th/h);
- Công TTĐT Cục QLTHADS (để đăng tải);
- Trang TTĐT THADS các tỉnh, thành phố (để đăng tải);
- Lưu: VT, TCTHADS.

**KT. BỘ TRƯỞNG
THỨ TRƯỞNG**



Mai Lương Khôi

QUY CHẾ

Bảo đảm an toàn thông tin, an ninh mạng cho các hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực thi hành án dân sự

(Ban hành kèm theo Quyết định số 2750/QĐ-BTP ngày 04 tháng 9 năm 2025 của Bộ trưởng Bộ Tư pháp)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh

Quy chế này quy định các chính sách quản lý và các biện pháp nhằm bảo đảm an toàn thông tin, an ninh mạng cho các hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực thi hành án dân sự (THADS).

2. Đối tượng áp dụng

a) Cục Quản lý THADS và các cơ quan THADS tham gia sử dụng, khai thác hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS;

b) Cơ quan, tổ chức, cá nhân tham gia kết nối, sử dụng, khai thác hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS;

c) Cơ quan, tổ chức, cá nhân tham gia cung cấp dịch vụ quản lý, vận hành, duy trì, phát triển mở rộng và bảo đảm an toàn thông tin mạng phục vụ hoạt động của hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS.

Điều 2. Giải thích từ ngữ

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

1. *An toàn thông tin mạng* là sự bảo vệ thông tin, hệ thống thông tin, phần mềm ứng dụng, Nền tảng số trong lĩnh vực THADS trên mạng tránh bị truy cập, 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. *Hạ tầng kỹ thuật* là tập hợp các thiết bị tính toán (máy chủ, máy trạm), thiết bị lưu trữ, thiết bị ngoại vi, thiết bị kết nối mạng, thiết bị phụ trợ, đường

truyền, mạng nội bộ, mạng diện rộng...

5. *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.

6. *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.

7. *Thiết bị đầu cuối* là các thiết bị như điện thoại cố định, điện thoại di động, máy tính, máy fax, USB, các thiết bị Bluetooth... có nhiệm vụ giải mã những tín hiệu và mã do tổng đài hoặc trung tâm chuyển mạch chuyển đến.

8. *Các thành phần của hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS*, bao gồm:

a) Hạ tầng kỹ thuật bao gồm thiết bị mạng, thiết bị/giải pháp an toàn thông tin, máy chủ ứng dụng, máy chủ cơ sở dữ liệu và các thiết bị phần cứng khác tại Trung tâm dữ liệu điện tử Bộ Tư pháp, đơn vị cung cấp dịch vụ công nghệ thông tin tham gia phục vụ cài đặt, vận hành, bảo đảm an toàn thông tin, an ninh mạng cho hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS;

b) Các phần mềm ứng dụng trong lĩnh vực THADS;

c) Cơ sở dữ liệu và các tập tin, dữ liệu của hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS.

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

1. Việc bảo đảm an toàn thông tin, an ninh mạng cho hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS phải tuân thủ các quy định của pháp luật về an toàn thông tin, an ninh mạng, bảo vệ bí mật nhà nước, bí mật công tác, thông tin, dữ liệu cá nhân và các quy định của Bộ Tư pháp có liên quan.

2. Việc tổ chức triển khai bảo đảm an toàn thông tin theo cấp độ cho hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục từ khâu thiết kế, xây dựng, trong quá trình vận hành, khai thác, nâng cấp, phát triển mở rộng, cho đến hủy bỏ hệ thống, tuân thủ các quy định tại 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 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 và Tiêu chuẩn quốc gia Việt Nam TCVN11930:2017 về công nghệ thông tin - các kỹ thuật an toàn - yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

3. Việc đầu tư, mua sắm, thuê các trang thiết bị, giải pháp phục vụ bảo đảm an toàn thông tin, an ninh mạng cho hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS phải được thực hiện một cách tổng thể, đồng bộ, tập trung, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp.

4. Các thông tin có nội dung bí mật nhà nước, phải thực hiện nghiêm theo quy định của Quy chế bảo vệ bí mật nhà nước của Bộ Tư pháp (ban hành kèm theo Quyết định số 1326/QĐ-BTP ngày 18/8/2021 của Bộ trưởng Bộ Tư pháp).

5. Cơ quan, tổ chức, cá nhân thuộc đối tượng áp dụng Quy chế này có trách nhiệm thực hiện bảo đảm an toàn thông tin, an ninh mạng cho hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS trong phạm vi chức năng, nhiệm vụ theo quy định của pháp luật, hướng dẫn của cơ quan, đơn vị có thẩm quyền và quy định tại Quy chế này.

Điều 4. Các hành vi bị nghiêm cấm

Tuân thủ quy định về các hành vi bị nghiêm cấm tại Điều 7 Luật An toàn thông tin mạng và Điều 8 Luật An ninh mạng.

Điều 5. Phối hợp với những cơ quan/tổ chức có thẩm quyền quản lý về an toàn thông tin và hỗ trợ điều phối xử lý sự cố an toàn thông tin

1. Cục Công nghệ thông tin:

a) Là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin và các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin phục vụ công tác bảo đảm an toàn thông tin, an ninh mạng và điều phối xử lý sự cố an toàn thông tin cho các hệ thống thông tin của Bộ Tư pháp trong đó có hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS.

b) Có trách nhiệm hướng dẫn, thông báo và phối hợp với Cục Quản lý THADS trong việc thực hiện bảo đảm an toàn thông tin, an ninh mạng và xử lý sự cố an toàn thông tin cho hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS.

2. Đơn vị cung cấp dịch vụ công nghệ thông tin

a) Cử đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin và các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin phục vụ công tác bảo đảm an toàn thông tin, an ninh mạng và điều phối xử lý sự cố an toàn thông tin cho các hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS trong quá trình cung cấp dịch vụ công nghệ thông tin.

b) Có trách nhiệm hướng dẫn, thông báo và phối hợp với Cục Quản lý THADS trong việc thực hiện bảo đảm an toàn thông tin, an ninh mạng và xử lý sự cố an toàn thông tin cho hệ thống thông tin, phần mềm ứng dụng và Nền tảng

số trong lĩnh vực THADS trong quá trình cung cấp dịch vụ công nghệ thông tin.

3. Cục Quản lý THADS:

a) Cử đầu mối phối hợp với Cục Công nghệ thông tin, đơn vị cung cấp dịch vụ công nghệ thông tin, chủ động, tích cực tham gia các hoạt động bảo đảm an toàn thông tin, an ninh mạng khi có yêu cầu;

b) Có trách nhiệm phối hợp với Cục Công nghệ thông tin trong việc xử lý các sự cố về an toàn thông tin, an ninh mạng đối với các thành phần của hệ thống thông tin, phần mềm ứng dụng được cài đặt tại Trung tâm dữ liệu điện tử Bộ Tư pháp; phối hợp với đơn vị cung cấp dịch vụ công nghệ thông tin trong việc xử lý các sự cố về an toàn thông tin, an ninh mạng đối với các thành phần của hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS khi sử dụng dịch vụ.

Chương II

BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ THIẾT KẾ, XÂY DỰNG HỆ THỐNG THÔNG TIN, PHẦN MỀM ỨNG DỤNG VÀ NỀN TẢNG SỐ TRONG LĨNH VỰC THADS

Điều 6. Thiết kế an toàn hệ thống thông tin

Trong quá trình thiết kế phục vụ xây dựng, nâng cấp, phát triển mở rộng hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS, đơn vị chủ trì thiết kế phải tuân thủ các quy định sau:

1. Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS.

2. Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS.

3. Có tài liệu mô tả phương án bảo đảm an toàn thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS theo cấp độ.

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

5. Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.

Điều 7. Phát triển phần mềm thuê khoán

Trong quá trình xây dựng, nâng cấp, phát triển mở rộng hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS, đối với các phần mềm thuê khoán (nếu có), yêu cầu các nhà phát triển phần mềm tuân thủ các quy định sau đây:

1. Có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán.

2. Cung cấp đầy đủ mã nguồn phần mềm.
3. Kiểm thử chức năng của phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.
4. Kiểm tra, đánh giá an toàn thông tin đối với hệ thống theo quy định tại khoản 3 Điều 12 Thông tư số 12/2022/TT-BTTTT trước khi đưa vào sử dụng.

Điều 8. Thử nghiệm và nghiệm thu hệ thống

Trong quá trình xây dựng, nâng cấp, phát triển mở rộng hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS, yêu cầu đơn vị chủ trì phối hợp với các nhà phát triển phần mềm phải tiến hành thử nghiệm và nghiệm thu hệ thống theo quy định tại Thông tư số 16/2024/TT-BTTTT ngày 30/12/2024 của Bộ Thông tin và Truyền thông quy định chi tiết nội dung công tác triển khai, giám sát công tác triển khai, nghiệm thu đối với dự án đầu tư ứng dụng công nghệ thông tin; xác định yêu cầu về chất lượng dịch vụ và các nội dung đặc thù của hợp đồng thuê dịch vụ đối với thuê dịch vụ công nghệ thông tin theo yêu cầu riêng, trong đó:

1. Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng, tuân thủ quy định tại Thông tư số 16/2024/TT-BTTTT.
2. Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống.
3. Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống.
4. Có đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống.
5. Có báo cáo nghiệm thu theo quy định tại Thông tư số 16/2024/TT-BTTTT, được xác nhận bởi bộ phận chuyên trách về công nghệ thông tin và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng.

Chương III

BẢO ĐẢM AN TOÀN THÔNG TIN TRONG QUẢN LÝ VẬN HÀNH HỆ THỐNG THÔNG TIN, PHẦN MỀM ỨNG DỤNG VÀ NỀN TẢNG SỐ TRONG LĨNH VỰC THI HÀNH ÁN DÂN SỰ

Điều 9. Quản lý nguồn nhân lực

1. Việc tuyển dụng nhân sự vị trí về an toàn thông tin tại đơn vị chuyên trách về an toàn thông tin hoặc đơn vị vận hành (nếu có) phải đảm bảo tuân thủ các quy định, quy trình tuyển dụng và điều kiện tuyển dụng được Bộ Tư pháp ban hành, có trình độ, chuyên ngành về công nghệ thông tin, an toàn thông tin phù hợp với vị trí tuyển dụng.

2. Trong quá trình làm việc:

a) Các cá nhân tham gia sử dụng hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS phải tuân thủ quy chế bảo đảm an toàn, an ninh thông tin mạng của Bộ Tư pháp (được ban hành kèm theo Quyết định số

45/QĐ-BTP ngày 16/01/2023);

b) Định kỳ hàng năm, Cục Quản lý THADS có kế hoạch tổ chức phổ biến, tuyên truyền, nâng cao nhận thức, đào tạo kỹ năng về an toàn thông tin cho công chức, viên chức và người lao động tại các đơn vị tham gia sử dụng hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS và cử công chức tham gia các lớp tập huấn về an toàn thông tin do Bộ Tư pháp tổ chức khi có yêu cầu.

3. Chấm dứt thay đổi công việc:

a) Khi có công chức, viên chức, người lao động chấm dứt hoặc thay đổi công việc, không tiếp tục tham gia sử dụng hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS, đơn vị quản lý công chức, viên chức, người lao động phải thu hồi tài khoản truy cập hệ thống và thông báo về Cục Quản lý THADS để vô hiệu hóa tài khoản;

b) Công chức, viên chức, người lao động chấm dứt hoặc thay đổi công việc, không tiếp tục tham gia sử dụng hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS phải chủ động bàn giao tài khoản truy cập hệ thống, bàn giao thông tin, dữ liệu lưu trên các thiết bị lưu trữ, các trang thiết bị, máy móc và các tài sản khác (nếu có) có liên quan đến hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS thuộc sở hữu của đơn vị; cam kết giữ bí mật thông tin liên quan đến hệ thống;

c) Cục Quản lý THADS thực hiện vô hiệu hóa tài khoản và tất cả các quyền truy cập tài nguyên, quản trị hệ thống sau khi công chức, viên chức, người lao động không tiếp tục tham gia sử dụng hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS.

Điều 10. Quản lý an toàn mạng

Tuân thủ các quy định về quản lý an toàn mạng tại Điều 15 Quy chế Bảo đảm an toàn, an ninh thông tin mạng của Trung tâm dữ liệu điện tử Bộ Tư pháp.

Điều 11. Quản lý an toàn máy chủ và ứng dụng

Tuân thủ các quy định về quản lý an toàn máy chủ và ứng dụng tại Điều 16 Quy chế Bảo đảm an toàn, an ninh thông tin mạng của Trung tâm dữ liệu điện tử Bộ Tư pháp.

Điều 12. Quản lý an toàn dữ liệu

Tuân thủ các quy định về quản lý an toàn dữ liệu tại Điều 17 Quy chế Bảo đảm an toàn, an ninh thông tin mạng của Trung tâm dữ liệu điện tử Bộ Tư pháp.

Điều 13. Quản lý an toàn thiết bị đầu cuối

Tuân thủ các quy định về quản lý an toàn thiết bị đầu cuối tại Điều 18 Quy chế Bảo đảm an toàn, an ninh thông tin mạng của Trung tâm dữ liệu điện tử Bộ Tư pháp.

Điều 14. Quản lý phòng chống phần mềm độc hại

Tuân thủ các quy định về quản lý an toàn thiết bị đầu cuối tại Điều 19 Quy chế Bảo đảm an toàn, an ninh thông tin mạng của Trung tâm dữ liệu điện tử Bộ Tư pháp.

Điều 15. Quản lý giám sát an toàn hệ thống thông tin

Tuân thủ các quy định về quản lý giám sát an toàn hệ thống thông tin tại Điều 20 Quy chế Bảo đảm an toàn, an ninh thông tin mạng của Trung tâm dữ liệu điện tử Bộ Tư pháp.

Điều 16. Quản lý điểm yếu an toàn thông tin

Tuân thủ các quy định về quản lý điểm yếu an toàn thông tin tại Điều 21 Quy chế Bảo đảm an toàn, an ninh thông tin mạng của Trung tâm dữ liệu điện tử Bộ Tư pháp.

Điều 17. Quản lý sự cố an toàn thông tin

Tuân thủ các quy định về quản lý sự cố an toàn thông tin tại Điều 22 Quy chế Bảo đảm an toàn, an ninh thông tin mạng của Trung tâm dữ liệu điện tử Bộ Tư pháp.

Điều 18. Quản lý an toàn người sử dụng đầu cuối

1. Kết nối máy tính/thiết bị đầu cuối của người sử dụng vào hệ thống:

a) Người sử dụng khi truy cập, sử dụng, khai thác thông tin của hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS phải tuân thủ các quy định của pháp luật và các quy định của đơn vị, tổ chức về bảo đảm an toàn thông tin;

b) Máy tính/thiết bị đầu cuối phải được xử lý điểm yếu an toàn thông tin, bảo mật trước khi truy cập vào hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS.

2. Trong quá trình sử dụng:

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ (nếu có) 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 quá trình kết nối, truy cập, sử dụng, khai thác thông tin của hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS;

b) Có trách nhiệm tự quản lý tài khoản và thiết bị được giao (nếu có) phục vụ vận hành, khai thác hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS;

c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay cho bộ phận có chuyên môn về công nghệ thông tin của đơn vị để kịp thời ngăn chặn và xử lý;

d) Đội ngũ thực hiện việc quản trị, vận hành hệ thống chủ động tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng do các đơn vị chuyên môn tổ chức.

Điều 19. Kiểm tra, đánh giá và quản lý rủi ro an toàn thông tin

Tuân thủ các quy định về quản lý điểm yếu an toàn thông tin tại Điều 24 Quy chế Bảo đảm an toàn, an ninh thông tin mạng của Trung tâm dữ liệu điện tử Bộ Tư pháp.

Điều 20. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

1. Yêu cầu thực hiện đối với việc kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin:

a) Thiết bị đầu cuối, thiết bị công nghệ thông tin khác có chứa dữ liệu khi bị hỏng phải được cán bộ kỹ thuật kiểm tra, đánh giá, ghi nhận để sửa chữa, khắc phục;

b) Trước khi tiến hành thanh lý/loại bỏ thiết bị công nghệ thông tin cũ, phải áp dụng các biện pháp kỹ thuật xóa bỏ hoàn toàn thông tin, dữ liệu đã lưu trữ, đảm bảo không thể phục hồi;

c) Các phương tiện và thiết bị công nghệ thông tin phục vụ quản trị, vận hành hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS, bao gồm: máy tính cá nhân, máy tính xách tay, máy chủ, các thiết bị lưu trữ như ổ cứng, thẻ nhớ, usb... phải xóa bỏ hoàn toàn thông tin, dữ liệu đã lưu trữ, đảm bảo không thể phục hồi khi chuyển giao hoặc thay đổi mục đích sử dụng.

2. Thực hiện kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin theo các quy định của pháp luật.

Chương IV TRÁCH NHIỆM CỦA TỔ CHỨC, CÁ NHÂN

Điều 21. Trách nhiệm Cục Quản lý THADS

1. Thực hiện trách nhiệm của đơn vị vận hành hệ thống thông tin theo quy định tại Điều 22 Nghị định số 85/2016/NĐ-CP và quy định của Quy chế này.

2. Tổ chức cài đặt, cấu hình hoạt động và triển khai hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS trong các cơ quan THADS đảm bảo hiệu quả, an toàn.

3. Chỉ đạo, phân công đơn vị chuyên môn thuộc Cục Quản lý THADS triển khai công tác bảo đảm an toàn thông tin của hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS.

4. Phối hợp với Cục Công nghệ thông tin xử lý các sự cố về an toàn thông tin, an ninh thông tin, bảo đảm hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS hoạt động thông suốt, an toàn và ổn định.

5. Hướng dẫn, phổ biến, triển khai việc thực hiện nội dung Quy chế này

và các quy định khác có liên quan đến toàn bộ công chức, viên chức và người lao động tại các đơn vị, cơ quan THADS; thường xuyên, đôn đốc, giám sát, kiểm tra, đánh giá việc tổ chức thực hiện Quy chế trong các Cơ quan THADS và kịp thời báo cáo Chủ quản hệ thống thông tin, Lãnh đạo Bộ Tư pháp các vấn đề vướng mắc phát sinh khi thực hiện Quy chế này.

Điều 22. Trách nhiệm Cục Công nghệ thông tin

1. Thực hiện trách nhiệm của đơn vị chuyên trách an toàn, an ninh thông tin mạng theo quy định tại Điều 21 Nghị định số 85/2016/NĐ-CP và quy định của Quy chế này.

2. Quản lý vận hành hạ tầng kỹ thuật Trung tâm dữ liệu điện tử của Bộ Tư pháp cung cấp môi trường hoạt động an toàn cho hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS.

3. Chủ trì, phối hợp với Cục Quản lý THADS xử lý các sự cố về an toàn, an ninh thông tin mạng của hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS, bảo đảm hệ thống hoạt động thông suốt, an toàn và ổn định.

Điều 23. Trách nhiệm đơn vị cung cấp dịch vụ công nghệ thông tin

1. Quản lý vận hành hạ tầng kỹ thuật cung cấp môi trường hoạt động an toàn cho hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS trong quá trình cung cấp dịch vụ công nghệ thông tin.

2. Chủ trì, phối hợp với Cục Quản lý THADS xử lý các sự cố về an toàn, an ninh thông tin mạng của hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS, bảo đảm hệ thống hoạt động thông suốt, an toàn và ổn định.

Điều 24. Trách nhiệm các cơ quan THADS tham gia sử dụng hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS

1. Tổ chức triển khai hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS trong phạm vi cơ quan đảm bảo hiệu quả, an toàn, tuân thủ quy định của Quy chế.

2. Phổ biến nội dung Quy chế này và các quy định khác có liên quan đến toàn bộ công chức, viên chức và người lao động tại cơ quan.

Điều 25. Trách nhiệm của các cá nhân tham gia sử dụng hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS

1. Thủ trưởng các Cơ quan THADS tham gia sử dụng hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS chịu trách nhiệm phổ biến nội dung Quy chế tới từng công chức, viên chức, người lao động của cơ quan; tổ chức triển khai và thường xuyên kiểm tra việc thực hiện Quy chế này tại cơ quan; chịu trách nhiệm trước pháp luật và Lãnh đạo Cục Quản lý THADS về các vi phạm Quy chế này của đơn vị do không tổ chức, chỉ đạo,

kiểm tra cán bộ của đơn vị thực hiện đúng quy định.

2. Công chức, viên chức, người lao động thuộc các Cơ quan THADS tham gia sử dụng hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS có trách nhiệm: tuân thủ Quy chế; thông báo các vấn đề bất thường liên quan tới an toàn hệ thống thông tin, phần mềm ứng dụng và Nền tảng số trong lĩnh vực THADS cho cơ quan và đơn vị vận hành hệ thống (Cục Quản lý THADS); chịu trách nhiệm trước pháp luật và Lãnh đạo Cơ quan THADS về các vi phạm Quy chế này.

Chương V **TỔ CHỨC THỰC HIỆN**

Điều 26. Tổ chức triển khai Quy chế

1. Cục trưởng Cục Quản lý THADS, Cục trưởng Cục Công nghệ thông tin có trách nhiệm phổ biến, quán triệt đến toàn bộ công chức, viên chức và người lao động trong cơ quan, đơn vị thực hiện các quy định của Quy chế này; thường xuyên kiểm tra việc thực hiện Quy chế này tại đơn vị; chịu trách nhiệm trước pháp luật và Lãnh đạo Bộ về các vi phạm, thất thoát thông tin, dữ liệu thuộc phạm vi quản lý của đơn vị do không tổ chức, chỉ đạo và kiểm tra cán bộ của đơn vị thực hiện đúng Quy chế.

2. Trong trường hợp các văn bản quy phạm pháp luật được dẫn chiếu tại Quy chế này được bãi bỏ, thay thế, sửa đổi, bổ sung thì thực hiện theo văn bản quy phạm pháp luật mới.

3. Hằng năm, Cục Quản lý THADS có trách nhiệm phối hợp với Cục Công nghệ thông tin rà soát nội dung Quy chế, kịp thời báo cáo Chủ quản hệ thống thông tin, Lãnh đạo Bộ Tư pháp các vấn đề vướng mắc phát sinh khi thực hiện Quy chế này; trình Bộ trưởng xem xét, quyết định việc sửa đổi, bổ sung nội dung Quy chế này cho phù hợp với tình hình thực tế và các quy định của pháp luật./.