BỘ TƯ PHÁP

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

QUY CHẾ
Quản lý, vận hành và sử dụng Nền tảng số trong lĩnh vực Thi hành án dân sự

(Ban hành kèm theo Quyết định số 882 /QĐ-BTP ngày 30 /03/2026 của Bộ Tư pháp)

Chương I: QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định về nguyên tắc, quản lý, vận hành, khai thác và sử dụng Nền tảng số trong lĩnh vực Thi hành án dân sự (sau đây gọi tắt là Nền tảng số THADS), bao gồm: quản lý truy cập và quản lý tài khoản người dùng; phân quyền, xác thực truy cập; vận hành kỹ thuật, bảo trì, chỉnh sửa, nâng cấp Nền tảng số THADS; cập nhật, quản lý, khai thác, trích xuất dữ liệu thi hành án dân sự; kết nối, tích hợp, chia sẻ dữ liệu nội bộ ngành và liên thông với các hệ thống thông tin khác; bảo đảm an toàn thông tin, an ninh mạng, bảo mật dữ liệu, bảo vệ dữ liệu cá nhân và quản lý, bảo vệ dữ liệu thuộc phạm vi bí mật nhà nước theo quy định của pháp luật; xử lý sự cố, sao lưu và phục hồi dữ liệu; trách nhiệm của các cơ quan, đơn vị, tổ chức, cá nhân có liên quan; kiểm tra, giám sát, tổ chức thực hiện và các hành vi bị nghiêm cấm trong quá trình quản lý, vận hành, khai thác và sử dụng Nền tảng số THADS

Điều 2. Đối tượng áp dụng

1. Các cơ quan thi hành án dân sự thuộc hệ thống thi hành án dân sự.

2. Công chức, người lao động thuộc hệ thống thi hành án dân sự được phân công sử dụng Nền tảng số THADS.

3. Cá nhân thuộc cơ quan có thẩm quyền theo quy định của pháp luật ngoài hệ thống thi hành án dân sự được cấp tài khoản sử dụng Nền tảng số THADS để phục vụ công tác quản lý, chỉ đạo, điều hành theo thẩm quyền.

4. Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS.

Điều 3. Giải thích từ ngữ

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

1. Nền tảng số THADS là hệ thống thông tin thống nhất phục vụ hoạt động quản lý, chỉ đạo, điều hành và nghiệp vụ thi hành án dân sự trên môi trường số, do Bộ Tư pháp tổ chức xây dựng, quản lý.

2. Người dùng là cá nhân được cấp tài khoản truy cập và sử dụng Nền tảng số THADS theo chức trách, nhiệm vụ được giao.

3. Tài khoản quản trị là tài khoản có quyền quản lý, phân quyền người dùng trên Nền tảng số THADS, bao gồm tài khoản quản trị cấp Cục và tài khoản quản trị cấp địa phương.

4. Dữ liệu thi hành án dân sự là toàn bộ thông tin, dữ liệu phát sinh trong quá trình tổ chức thi hành án dân sự được cập nhật, lưu trữ, quản lý trên Nền tảng số THADS.

5. Dữ liệu cá nhân là thông tin dưới dạng ký hiệu, chữ viết, số, hình ảnh, âm thanh hoặc dạng tương tự trên môi trường điện tử gắn liền với một cá nhân cụ thể hoặc giúp xác định một cá nhân cụ thể, theo quy định của pháp luật về bảo vệ dữ liệu cá nhân.

6. Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS là đơn vị được giao vận hành kỹ thuật, bảo trì, hỗ trợ và bảo đảm hoạt động của Nền tảng số THADS theo hợp đồng ký kết với Cục Quản lý THADS.

Điều 4. Nguyên tắc quản lý, vận hành, khai thác và sử dụng Nền tảng số THADS

1. Việc quản lý, vận hành, khai thác và sử dụng Nền tảng số THADS phải được thực hiện thống nhất, đúng thẩm quyền, tuân thủ đầy đủ các quy định của pháp luật về thi hành án dân sự, công nghệ thông tin, an toàn thông tin mạng, bảo vệ dữ liệu cá nhân và các quy định pháp luật có liên quan.

2. Nền tảng số THADS được sử dụng đúng mục đích phục vụ hoạt động công vụ trong lĩnh vực thi hành án dân sự; mọi hoạt động khai thác, cập nhật, chia sẻ và sử dụng dữ liệu trên Nền tảng số THADS phải bảo đảm đúng chức năng, nhiệm vụ, quyền hạn của cơ quan, đơn vị, cá nhân theo quy định.

3. Dữ liệu trên Nền tảng số THADS phải được cập nhật, quản lý tập trung, thống nhất; bảo đảm tính chính xác, đầy đủ, kịp thời và nhất quán. Việc quản lý, khai thác và sử dụng dữ liệu phải bảo đảm an toàn, bảo mật thông tin trong toàn bộ quá trình tạo lập, lưu trữ, truyền đưa, cập nhật và sử dụng.

4. Nền tảng số THADS được xây dựng, quản lý và vận hành bảo đảm phù hợp với Khung kiến trúc dữ liệu quốc gia và Khung kiến trúc Chính phủ số. Dữ liệu của hệ thống cần được tổ chức theo các nguyên tắc chuẩn hóa, định danh thống nhất, bảo đảm khả năng kết nối, tích hợp và chia sẻ với các hệ thống thông tin của bộ, ngành và Cơ sở dữ liệu tổng hợp quốc gia thông qua các nền tảng tích hợp, chia sẻ dữ liệu theo quy định của Chính phủ.

5. Trách nhiệm của từng cơ quan, đơn vị, cá nhân trong việc quản lý, vận hành và sử dụng Nền tảng số THADS được quy định cụ thể, rõ ràng; đồng thời tăng cường công tác kiểm tra, giám sát, kiểm soát nội bộ nhằm bảo đảm Nền tảng số THADS được vận hành thông suốt, hiệu quả, đúng quy định của pháp luật.

Điều 5. Các hành vi bị nghiêm cấm

1. Nghiêm cấm các cơ quan, tổ chức, cá nhân có liên quan trong phạm vi điều chỉnh của Quy chế này thực hiện các hành vi sau đây:

2. Thực hiện các hành vi bị nghiêm cấm theo quy định của pháp luật về công nghệ thông tin, chuyển đổi số, an toàn thông tin mạng, an ninh mạng, tiếp

cận thông tin, bảo vệ bí mật nhà nước, giao dịch điện tử, bảo vệ dữ liệu cá nhân và các văn bản quy phạm pháp luật khác có liên quan.

3. Cấp phát tài khoản, phân quyền truy cập hoặc cho phép sử dụng Nền tảng số THADS đối với cơ quan, tổ chức, cá nhân không thuộc đối tượng, điều kiện được cấp theo quy định.

4. Tự ý sao chép, cung cấp, chuyển giao, tiết lộ, công khai thông tin, dữ liệu thuộc Nền tảng số THADS, bao gồm dữ liệu cá nhân và dữ liệu nghiệp vụ thi hành án dân sự, cho cơ quan, tổ chức, cá nhân không có trách nhiệm hoặc không có thẩm quyền tiếp cận theo quy định.

5. Tự ý xóa, sửa đổi, làm sai lệch, hủy hoại, phá hoại dữ liệu được lưu trữ trên Nền tảng số THADS; tự ý thay đổi, thu hồi, xóa bỏ hoặc can thiệp vào quyền truy cập của người dùng khi chưa được cơ quan, người có thẩm quyền cho phép.

6. Lưu trữ, khai thác, sử dụng trái phép dữ liệu trên Nền tảng số THADS (bao gồm dữ liệu cá nhân) nhằm mục đích xâm hại lợi ích của Nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc nhằm mục đích vụ lợi.

7. Truy cập trái phép; tìm cách vượt quyền truy cập; xâm nhập, can thiệp, phá hoại hệ thống; thực hiện hành vi tấn công mạng, phát tán phần mềm độc hại hoặc các hành vi khác gây gián đoạn, làm sai lệch, thay đổi, xóa, hủy dữ liệu hoặc làm ảnh hưởng đến hoạt động an toàn, ổn định của Nền tảng số THADS.

8. Khai thác, sử dụng dữ liệu vượt quá phạm vi thẩm quyền được giao; cản trở trái pháp luật, gây cản trở hoặc làm gián đoạn hoạt động bình thường của Nền tảng số THADS và các hệ thống thông tin có liên quan.

9. Sử dụng trái phép danh tính điện tử, chứng thư số, mã định danh; can thiệp, làm sai lệch cơ chế xác thực, định danh người dùng trên Nền tảng số THADS; thực hiện các hành vi vi phạm quy định về định danh và xác thực điện tử theo Nghị định số 59/2022/NĐ-CP và các quy định pháp luật hiện hành.

10. Vi phạm các quy định về bảo đảm an toàn thông tin mạng; cố ý làm lộ, lọt, chiếm đoạt, sử dụng trái phép thông tin thuộc bí mật nhà nước, thông tin mật của cơ quan, đơn vị; vi phạm quy định về bảo vệ dữ liệu cá nhân trong quá trình quản lý, vận hành và sử dụng Nền tảng số THADS.

11. Sử dụng Nền tảng số THADS, tài khoản, thiết bị, phương tiện được cấp để phục vụ vào mục đích cá nhân hoặc các hoạt động không liên quan đến chức năng, nhiệm vụ được giao; cho mượn, cho thuê, chia sẻ tài khoản, thiết bị cho người không có thẩm quyền để sử dụng trái phép.

Chương II: QUẢN LÝ TRUY CẬP, PHÂN QUYỀN NGƯỜI DÙNG

Điều 6. Truy cập Nền tảng số THADS

Nền tảng số THADS được truy cập thống nhất thông qua tên miền chính thức: https://ntsthads.moj.gov.vn/ và chỉ được khai thác, sử dụng bởi các cơ quan,

tổ chức, cá nhân có tài khoản người dùng đã được cấp có thẩm quyền cấp theo quy định của Quy chế này. Trường hợp thay đổi, bổ sung tên miền truy cập Nền tảng số THADS, Cục Quản lý THADS có trách nhiệm xem xét, quyết định và thông báo chính thức bằng văn bản hoặc trên các kênh thông tin chính thức để các cơ quan, đơn vị, cá nhân có liên quan biết, thực hiện thống nhất.

Điều 7. Quản lý tài khoản người dùng

1. Việc cấp phát tài khoản truy cập Nền tảng số THADS phải bảo đảm đúng đối tượng, đúng điều kiện và đúng thẩm quyền theo quy định của Quy chế này. Chỉ cá nhân thuộc đối tượng được phép, đáp ứng yêu cầu về chức năng, nhiệm vụ mới được xem xét, cấp tài khoản truy cập.

2. Mỗi người dùng chỉ được cấp một (01) tài khoản riêng biệt và phải chịu trách nhiệm trước pháp luật, trước cơ quan, đơn vị quản lý về toàn bộ hoạt động phát sinh dưới tài khoản được cấp.

3. Cục Quản lý THADS là cơ quan có thẩm quyền xem xét, phê duyệt việc cấp mới, điều chỉnh, khóa và thu hồi tài khoản truy cập Nền tảng số THADS theo đúng trình tự, thủ tục quy định tại Quy chế này.

4. Tài khoản quản trị (admin) tại Cơ quan THADS địa phương được thực hiện các thao tác kỹ thuật về phân quyền, tạo mới, khóa hoặc thu hồi tài khoản người dùng trong phạm vi cơ quan, đơn vị mình quản lý, phù hợp với các nhóm quyền và chức năng đã được thiết lập trên Nền tảng số THADS. Việc phân quyền, tạo mới, khóa hoặc thu hồi tài khoản chỉ có hiệu lực chính thức sau khi được tài khoản quản trị của Cục Quản lý THADS phê duyệt trên hệ thống.

Trường hợp người dùng nghỉ việc, chuyển công tác, chấm dứt nhiệm vụ, thay đổi vị trí công tác hoặc không còn nhu cầu sử dụng Nền tảng số THADS, cơ quan, đơn vị quản lý trực tiếp có trách nhiệm kịp thời đề nghị và phối hợp thực hiện việc khóa hoặc thu hồi tài khoản theo quy trình quản trị hai cấp quy định tại Điều 9 của Quy chế này.

5. Cơ quan, đơn vị và cá nhân được cấp tài khoản có trách nhiệm quản lý, bảo mật thông tin tài khoản theo quy định. Người dùng phải giữ bí mật mật khẩu; khi phát hiện tài khoản có dấu hiệu bị lộ, mất an toàn hoặc bị truy cập trái phép, phải kịp thời thông báo cho bộ phận quản trị hệ thống để kiểm tra, xử lý theo quy định.

6. Danh sách và thông tin chi tiết về các tài khoản người dùng (bao gồm thông tin phân quyền) phải được bộ phận quản trị hệ thống cập nhật đầy đủ, chính xác và lưu trữ an toàn. Mọi thay đổi về trạng thái tài khoản (cấp mới, điều chỉnh, khóa, thu hồi, thay đổi quyền truy cập) phải được ghi nhận vào nhật ký quản trị hệ thống. Nhật ký quản trị là căn cứ phục vụ công tác kiểm tra, giám sát, kiểm soát truy cập và xử lý khi xảy ra sự cố về an toàn, an ninh thông tin. Cục Quản lý THADS là đơn vị quản lý nhật ký quản trị; Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS có trách nhiệm bảo đảm chức năng kỹ thuật phục vụ việc ghi nhận, lưu trữ, trích xuất nhật ký theo yêu cầu của cơ quan có thẩm quyền.

7. Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS chịu trách nhiệm phát triển, duy trì các chức năng kỹ thuật liên quan đến việc tạo lập tài khoản, phân quyền, điều chỉnh, khóa và thu hồi tài khoản; bảo đảm việc thực hiện đúng thẩm quyền, đúng quy định của Quy chế này và đáp ứng các yêu cầu về an toàn, bảo mật thông tin. Không được tự ý thay đổi, cấp phát hoặc điều chỉnh quyền truy cập khi chưa có ý kiến phê duyệt của cơ quan có thẩm quyền.

Điều 8. Phân quyền và xác thực người dùng

1. Mỗi tài khoản người dùng được phân cấp quyền hạn tương ứng với chức trách, nhiệm vụ được giao. Việc phân quyền phải bảo đảm nguyên tắc quyền hạn tối thiểu, theo đó người dùng chỉ được truy cập những chức năng, dữ liệu cần thiết cho công việc được giao. Cục Quản lý THADS chịu trách nhiệm thiết lập và quản lý hệ thống phân quyền trên toàn Nền tảng số THADS. Theo mô hình phân cấp, có hai cấp tài khoản quản trị và các nhóm tài khoản người dùng, gồm:

a) Tài khoản quản trị cấp Cục (Admin Cục) là tài khoản do Cục Quản lý THADS quản lý, có thẩm quyền phê duyệt các thao tác quản lý tài khoản do Admin địa phương thực hiện; tạo, điều chỉnh, khóa, thu hồi tài khoản quản trị cấp địa phương và các tài khoản người dùng khác theo phân cấp; quản lý, giám sát toàn bộ hệ thống tài khoản trên Nền tảng số THADS.

b) Tài khoản quản trị cấp địa phương (Admin địa phương) là tài khoản do Cơ quan THADS địa phương quản lý, được sử dụng để thực hiện các thao tác kỹ thuật về tạo lập, điều chỉnh thông tin, phân quyền, khóa, đề nghị thu hồi tài khoản người dùng thuộc phạm vi quản lý của đơn vị.

c) Tài khoản người dùng trong hệ thống THADS là tài khoản được cấp cho công chức, người lao động trong hệ thống thi hành án dân sự để thực hiện các nghiệp vụ theo chức trách, nhiệm vụ được giao.

d) Tài khoản người dùng ngoài hệ thống THADS là tài khoản được cấp cho cá nhân thuộc cơ quan có thẩm quyền theo quy định của pháp luật ngoài hệ thống thi hành án dân sự để phục vụ công tác quản lý, chỉ đạo, điều hành theo thẩm quyền; phạm vi truy cập, khai thác dữ liệu của nhóm tài khoản này phải được giới hạn theo đúng chức năng, nhiệm vụ và thẩm quyền được giao.

2. Tài khoản người dùng trên Nền tảng số THADS phải được bảo vệ bằng mật khẩu đáp ứng yêu cầu bảo mật cao như sau:

a) Mật khẩu người dùng phải có độ dài tối thiểu 8 ký tự, mật khẩu của tài khoản quản trị hệ thống tối thiểu 12 ký tự. Mật khẩu không chứa các thông tin dễ đoán. Đối với mật khẩu tài khoản quản trị, bắt buộc phải bao gồm kết hợp cả chữ thường, chữ in hoa, chữ số và ký tự đặc biệt.

b) Mật khẩu tài khoản người dùng phải được thay đổi định kỳ ít nhất 6 tháng một lần; riêng mật khẩu tài khoản quản trị hệ thống (admin) phải thay đổi tối thiểu 3 tháng một lần. Hệ thống phải có chức năng nhắc nhở người dùng đổi mật khẩu định kỳ.

c) Người được cấp tài khoản phải đổi mật khẩu mặc định ngay lần đăng nhập đầu tiên và bảo mật mật khẩu trong suốt quá trình sử dụng. Mật khẩu quản trị hệ thống sau khi đổi cần được lưu trữ an toàn và chỉ cấp cho quản trị viên có trách nhiệm.

d) Đối với các tài khoản có quyền hạn cao, bắt buộc áp dụng phương thức xác thực đa yếu tố (như mã OTP, chứng thư số) để tăng cường bảo mật truy cập. Trường hợp Nền tảng số THADS tích hợp với Nền tảng định danh và xác thực điện tử quốc gia (VNeID) hoặc dịch vụ xác thực tập trung, việc xác thực người dùng sẽ tuân theo cơ chế do hệ thống đó quy định, đồng thời phù hợp với Nghị định về định danh và xác thực điện tử hiện hành.

Điều 9. Cấp mới, thay đổi, khóa và thu hồi tài khoản

1. Việc cấp mới, thay đổi, khóa hoặc thu hồi tài khoản người dùng được thực hiện theo mô hình quản trị hai cấp (Admin địa phương và Admin Cục) thông qua chức năng quản lý tài khoản được tích hợp trên Nền tảng số THADS.

2. Khi phát sinh nhu cầu cấp mới, thay đổi, khóa hoặc thu hồi tài khoản người dùng, Admin địa phương thực hiện đầy đủ các thao tác cấu hình tài khoản trên Nền tảng số THADS theo đúng phạm vi quản lý, bao gồm tạo tài khoản, chỉnh sửa thông tin, phân quyền, gán vai trò, khóa hoặc thu hồi tài khoản. Các thao tác này được hệ thống ghi nhận ở trạng thái chờ phê duyệt và tự động chuyển thông tin đến Admin Cục để xem xét, quyết định. Các thao tác quản lý tài khoản do Admin địa phương thực hiện chỉ phát sinh hiệu lực sau khi được Admin Cục phê duyệt trên hệ thống.

Trường hợp chưa được phê duyệt, tài khoản chưa có hiệu lực truy cập và sử dụng Nền tảng số THADS.

Trường hợp không được phê duyệt, hệ thống ghi nhận lý do từ chối và thông báo cho Admin địa phương để xử lý theo quy định.

Toàn bộ quá trình thực hiện, phê duyệt hoặc từ chối cấp mới, thay đổi, khóa hoặc thu hồi tài khoản được thực hiện hoàn toàn trên Nền tảng số THADS trong thời hạn 01 ngày làm việc kể từ khi khởi tạo yêu cầu.

Chương III: VẬN HÀNH KỸ THUẬT NỀN TẢNG SỐ THADS

Điều 10. Yêu cầu vận hành và bảo trì kỹ thuật

1. Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS có trách nhiệm vận hành hệ thống bảo đảm hoạt động liên tục, ổn định và an toàn. Các thành phần hạ tầng như máy chủ, hệ thống mạng, cơ sở dữ liệu… phải được giám sát 24/7 và có biện pháp dự phòng để nhanh chóng khôi phục khi xảy ra sự cố. Mọi hoạt động bảo trì, nâng cấp, thay thế thiết bị cần được lên kế hoạch cụ thể, hạn chế tối đa ảnh hưởng tới sự hoạt động của Nền tảng số THADS.

2. Hệ thống phải được thiết lập cơ chế giám sát cảnh báo sớm (về hiệu năng, lỗi phần cứng, phần mềm, tấn công mạng…). Quản trị viên kỹ thuật phải thường

xuyên theo dõi trạng thái các máy chủ, thiết bị mạng, ứng dụng; kịp thời xử lý hoặc báo cáo khi phát hiện dấu hiệu bất thường (quá tải, lỗi, truy cập trái phép…). Thực hiện bảo trì định kỳ, bao gồm kiểm tra, vệ sinh thiết bị, cập nhật bản vá phần mềm, thay thế phần cứng hỏng, để bảo đảm hệ thống luôn hoạt động ổn định.

3. Các máy chủ, thiết bị mạng, thiết bị bảo mật… thuộc Nền tảng số THADS cần được cập nhật kịp thời các bản vá lỗi hệ thống, bản vá lỗ hổng bảo mật từ nhà cung cấp. Khi có cảnh báo về lỗ hổng an ninh mạng từ cơ quan chức năng, đơn vị vận hành phải nhanh chóng thực hiện các biện pháp khắc phục, vá lỗi để phòng ngừa nguy cơ bị tấn công. Đồng thời, thường xuyên cập nhật mẫu nhận diện mã độc cho các phần mềm phòng chống virus/malware trên hệ thống.

4. Toàn bộ quá trình vận hành, bảo trì hệ thống phải được ghi chép vào nhật ký vận hành kỹ thuật. Nội dung ghi bao gồm thời gian, người thực hiện, hạng mục công việc (kiểm tra, cấu hình, thay thế linh kiện, cập nhật phần mềm...), kết quả thực hiện và các ghi chú cần thiết. Nhật ký này được lưu giữ tại Cục Quản lý THADS và tại Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS trong thời hạn tối thiểu 02 năm. Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS có trách nhiệm cung cấp nhật ký khi có yêu cầu của cơ quan có thẩm quyền hoặc khi phát sinh sự cố phục vụ công tác quản lý, kiểm tra, giám sát.

Điều 11. Chỉnh sửa, nâng cấp Nền tảng số THADS

1. Việc chỉnh sửa, nâng cấp quy trình nghiệp vụ và các chức năng trên Nền tảng số THADS được thực hiện khi có một trong các căn cứ sau:

a) Phát sinh nghiệp vụ mới trong hoạt động thi hành án dân sự;

b) Có sự thay đổi, bổ sung của quy định pháp luật liên quan;

c) Yêu cầu cải tiến, hoàn thiện tính năng kỹ thuật nhằm đáp ứng yêu cầu thực tiễn sử dụng của người dùng;

d) Khắc phục hạn chế, bất cập phát sinh trong quá trình vận hành, khai thác Nền tảng số THADS.

2. Cục Quản lý THADS là đầu mối tiếp nhận các kiến nghị, đề xuất của người dùng, các Cơ quan THADS địa phương và các đơn vị liên quan về việc chỉnh sửa, nâng cấp quy trình nghiệp vụ hoặc chức năng của Nền tảng số THADS. Các kiến nghị, đề xuất phải được gửi bằng văn bản hoặc thông qua kênh tiếp nhận chính thức do Cục Quản lý THADS công bố, nêu rõ nội dung đề xuất, lý do, phạm vi ảnh hưởng và yêu cầu mong muốn (nếu có).

3. Cục Quản lý THADS có trách nhiệm chủ trì tổng hợp, rà soát và đánh giá các kiến nghị, đề xuất; đồng thời phân loại yêu cầu theo tính chất, bao gồm:

a) Yêu cầu chỉnh sửa, bổ sung chức năng liên quan trực tiếp đến quy trình nghiệp vụ, biểu mẫu sử dụng trong thi hành án dân sự;

b) Yêu cầu nâng cấp, bổ sung tính năng kỹ thuật, tiện ích, trải nghiệm người dùng, không làm thay đổi bản chất quy trình nghiệp vụ;

c) Yêu cầu khắc phục lỗi kỹ thuật, bất cập trong quá trình vận hành Nền tảng số THADS.

d) Đối với các nội dung liên quan đến nghiệp vụ thi hành án dân sự, các Ban nghiệp vụ thuộc Cục Quản lý THADS có trách nhiệm phối hợp với Ban chuyển đổi số và Thống kê dữ liệu và Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS rà soát, thống nhất yêu cầu nghiệp vụ, phương án chỉnh sửa, bảo đảm phù hợp với quy định pháp luật và quy trình nghiệp vụ hiện hành trước khi triển khai thực hiện. Đối với các nội dung nâng cấp tính năng kỹ thuật, tiện ích cho người dùng, Ban chuyển đổi số và Thống kê dữ liệu thuộc Cục Quản lý THADS là đơn vị chủ trì, phối hợp với Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS xây dựng phương án nâng cấp, tổ chức triển khai thực hiện theo thẩm quyền.

Điều 12. Sao lưu và phục hồi dữ liệu

1. Dữ liệu trên Nền tảng số THADS phải được sao lưu dự phòng thường xuyên nhằm phòng ngừa mất mát dữ liệu. Tối thiểu thực hiện sao lưu hằng ngày (sao lưu gia tăng đối với các dữ liệu thay đổi trong ngày), hằng tuần (sao lưu toàn bộ dữ liệu) và hằng tháng (lưu trữ một bản sao lưu toàn bộ dữ liệu định kỳ phục vụ lưu trữ dài hạn). Việc sao lưu có thể thực hiện tự động bằng phần mềm chuyên dụng hoặc thủ công, nhưng phải bảo đảm mọi dữ liệu quan trọng đều được sao lưu đầy đủ. Mỗi lần sao lưu phải ghi nhận nhật ký sao lưu dữ liệu, thể hiện rõ thời gian, phương thức sao lưu, thành phần dữ liệu được sao lưu, người thực hiện và tình trạng của bản sao lưu.

2. Dữ liệu sau khi sao lưu phải được lưu giữ tại khu vực an toàn. Ít nhất một bản sao lưu đầy đủ cần được lưu tại địa điểm khác với trung tâm dữ liệu chính để phòng trường hợp thảm họa tại chỗ. Các bản sao lưu phải được bảo mật (mã hóa nếu trên thiết bị số, niêm phong nếu trên thiết bị vật lý) và được quản lý phân quyền truy cập chặt chẽ.

3. Bản sao lưu được lưu trữ trong thời gian tối thiểu theo quy định về lưu trữ hồ sơ, tài liệu của ngành và pháp luật về lưu trữ hiện hành. Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS định kỳ kiểm tra tính toàn vẹn của các bản sao lưu và thực hiện phục hồi thử nghiệm từ bản sao lưu để đảm bảo dữ liệu sao lưu có thể phục hồi thành công khi cần thiết.

4. Khi xảy ra sự cố mất dữ liệu trên Nền tảng số THADS, Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS phải khẩn trương đánh giá mức độ và phạm vi ảnh hưởng, báo cáo Bộ Tư pháp, Cục Quản lý THADS; đồng thời thực hiện quy trình phục hồi dữ liệu từ bản sao lưu gần nhất. Quá trình phục hồi phải đảm bảo dữ liệu được khôi phục đầy đủ, nhất quán và hệ thống hoạt động bình thường trở lại trong thời gian ngắn nhất. Sau phục hồi, cần phân tích nguyên nhân sự cố để có biện pháp phòng ngừa trong tương lai.

Điều 13. Quản lý sự cố và hỗ trợ kỹ thuật

1. Cục Quản lý THADS là đầu mối quản lý, tổng hợp và theo dõi việc tiếp nhận, xử lý sự cố đối với Nền tảng số THADS. Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS là đầu mối hỗ trợ kỹ thuật trực tiếp 24/7, có trách nhiệm công khai số điện thoại đường dây nóng, địa chỉ thư điện tử hỗ trợ và các kênh tiếp nhận thông tin sự cố khác. Khi có sự cố về Nền tảng số THADS, người dùng và đơn vị liên quan phải kịp thời thông báo cho đầu mối hỗ trợ kỹ thuật của Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS để được hướng dẫn, xử lý; đồng thời thông tin cho Cục Quản lý THADS để theo dõi, chỉ đạo trong trường hợp cần thiết.

2. Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS phải xây dựng quy trình cụ thể để ứng phó các loại sự cố (sự cố phần cứng, phần mềm, mất kết nối, tấn công mạng, rò rỉ dữ liệu...). Khi xảy ra sự cố, quản trị kỹ thuật cần ngay lập tức đánh giá mức độ nghiêm trọng và thực hiện các biện pháp khoanh vùng, ngăn chặn nhằm tránh thiệt hại lan rộng. Đồng thời, báo cáo Lãnh đạo đơn vị và thông báo cho các bên liên quan biết về sự cố. Đối với sự cố nghiêm trọng phải phối hợp khắc phục trong vòng 24 giờ kể từ khi phát hiện.

3. Trường hợp sự cố liên quan đến an toàn thông tin (tấn công mạng, xâm nhập trái phép, phát hiện mã độc nguy hiểm, rò rỉ dữ liệu nhạy cảm...), Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS phải phối hợp chặt chẽ với các cơ quan chức năng về an ninh mạng; thông báo ngay cho đơn vị chuyên trách về Công nghệ thông tin thuộc Bộ Tư pháp và Cục Quản lý THADS tùy tính chất sự cố; đồng thời thực hiện các biện pháp ứng cứu theo chỉ đạo của cơ quan chức năng. Việc xử lý sự cố an ninh mạng phải tuân thủ quy định của Luật An ninh mạng 2018 và phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia. Trong quá trình khắc phục, cần giám sát hệ thống liên tục để đề phòng sự cố tái diễn hoặc lợi dụng tấn công lần hai.

4. Mọi sự cố quan trọng sau khi xử lý xong phải được lập báo cáo sự cố gửi Cục Quản lý THADS. Báo cáo nêu rõ thời gian, diễn biến, nguyên nhân, thiệt hại (nếu có), cách thức khắc phục và các biện pháp đã, sẽ triển khai để ngăn ngừa lặp lại. Đồng thời, các bài học kinh nghiệm từ sự cố cần được rút ra và phổ biến tới các quản trị viên liên quan. Trường hợp sự cố gây ảnh hưởng lớn, Cục Quản lý THADS có trách nhiệm thông báo tới cơ quan quản lý cấp trên và các bên bị ảnh hưởng, tuân thủ quy định pháp luật.

CHƯƠNG IV

CẬP NHẬT, KHAI THÁC DỮ LIỆU THI HÀNH ÁN DÂN SỰ

Điều 14. Nguyên tắc cập nhật và bảo đảm chất lượng dữ liệu thi hành án dân sự

1. Dữ liệu trên Nền tảng số THADS phải được cập nhật bảo đảm đầy đủ, chính xác, kịp thời, đúng trình tự nghiệp vụ và đúng thẩm quyền.

2. Dữ liệu phát sinh tại khâu nghiệp vụ nào thì được cập nhật tại khâu nghiệp vụ đó; bảo đảm dữ liệu thống nhất, có mã định danh theo quy định, không trùng lặp, không sai lệch, không mâu thuẫn giữa các trường thông tin.

3. Việc cập nhật dữ liệu phải tuân thủ chuẩn dữ liệu, danh mục dùng chung, biểu mẫu và quy trình nghiệp vụ do cơ quan có thẩm quyền ban hành; các trường thông tin bắt buộc phải được cập nhật đầy đủ theo quy định.

4. Thời hạn cập nhật dữ liệu

a) Thông tin phát sinh từ hoạt động nghiệp vụ bên ngoài mà không thể sử dụng trực tiếp Nền tảng số THADS phải được cập nhật lên Nền tảng số THADS chậm nhất trong 01 ngày làm việc kể từ thời điểm phát sinh (trừ trường hợp quy định chuyên ngành có thời hạn khác);

b) Trường hợp hệ thống gặp sự cố hoặc bất khả kháng, việc cập nhật được thực hiện ngay khi hệ thống hoạt động bình thường; đơn vị phải ghi nhận và lưu vết nguyên nhân chậm cập nhật (nếu có).

5. Kiểm soát chất lượng và xử lý sai sót:

a) Nền tảng số THADS áp dụng các cơ chế kiểm tra/đối soát dữ liệu (cảnh báo thiếu trường bắt buộc, cảnh báo trùng lặp, cảnh báo sai logic…); người dùng và đơn vị có trách nhiệm xử lý các cảnh báo theo thẩm quyền;

b) Việc sửa đổi, đính chính dữ liệu phải có lý do, người thực hiện, và được lưu nhật ký trên hệ thống; trường hợp sửa đổi làm thay đổi bản chất thông tin nghiệp vụ thì phải thực hiện theo đúng thẩm quyền và quy trình nghiệp vụ được ban hành.

c) Người đứng đầu cơ quan thi hành án dân sự chịu trách nhiệm về chất lượng dữ liệu do đơn vị mình tạo lập, cập nhật trên Nền tảng số THADS; đồng thời tổ chức kiểm tra, rà soát thường xuyên theo cơ chế đối soát dữ liệu với hồ sơ, tài liệu tác nghiệp thực tế để kịp thời phát hiện và khắc phục sai sót.

Điều 15. Khai thác, sử dụng và trích xuất dữ liệu thi hành án dân sự

1. Việc khai thác, sử dụng dữ liệu trên Nền tảng số THADS phải phục vụ công tác quản lý, chỉ đạo, điều hành và nghiệp vụ thi hành án dân sự, đúng chức năng, nhiệm vụ, quyền hạn của cơ quan, đơn vị và cá nhân.

Người dùng chỉ được khai thác dữ liệu trong phạm vi tài khoản, vai trò và quyền được phân quyền; phải tuân thủ nguyên tắc đúng mục đích, tối thiểu quyền và bảo mật thông tin theo quy định.

2. Nghiêm cấm việc khai thác, sao chép, cung cấp, chia sẻ dữ liệu cho tổ chức, cá nhân không có thẩm quyền; nghiêm cấm sử dụng dữ liệu vào mục đích ngoài nhiệm vụ hoặc trái quy định của pháp luật.

3. Việc trích xuất dữ liệu để phục vụ báo cáo, thống kê, kiểm tra, đối soát phải tuân thủ biểu mẫu, định dạng, quy trình do cơ quan có thẩm quyền ban hành;

đồng thời bảo đảm lưu vết việc trích xuất (thời gian, người thực hiện, phạm vi dữ liệu, mục đích).

Chương V: KẾT NỐI, CHIA SẺ DỮ LIỆU

Điều 16. Kết nối và chia sẻ dữ liệu với các hệ thống thông tin khác

1. Nền tảng số THADS đóng vai trò là hệ thống dùng chung trong toàn Hệ thống Thi hành án dân sự, cần được kết nối với các phần mềm nghiệp vụ chuyên ngành khác (nếu có) để đồng bộ và chia sẻ dữ liệu phục vụ công tác quản lý, chỉ đạo điều hành. Việc kết nối nội bộ phải đảm bảo thông suốt, dữ liệu thống nhất, tránh nhập liệu trùng lặp. Các danh mục dùng chung (như danh mục đơn vị hành chính, chức danh, trạng thái việc thi hành án…) phải được sử dụng thống nhất giữa các hệ thống để bảo đảm tích hợp dữ liệu đồng bộ, chính xác.

2. Trường hợp cần chia sẻ, trao đổi dữ liệu giữa Nền tảng số THADS với các hệ thống thông tin của Bộ, Ngành khác, việc kết nối phải thực hiện thông qua các nền tảng tích hợp dữ liệu theo quy định chung, ưu tiên sử dụng Nền tảng tích hợp, chia sẻ dữ liệu quốc gia (NDXP) và Nền tảng tích hợp, chia sẻ dữ liệu Bộ, ngành, địa phương (LGSP) để thực hiện kết nối liên thông giữa Nền tảng số THADS với các hệ thống bên ngoài. Mọi kết nối, chia sẻ phải tuân thủ quy định về quản lý, kết nối và chia sẻ dữ liệu số giữa các cơ quan nhà nước.

3. Trước khi thực hiện kết nối, Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS, Ban chuyển đổi số và Thống kê dữ liệu thuộc Cục Quản lý THADS phối hợp với đơn vị quản lý hệ thống thông tin cần chia sẻ thống nhất các yêu cầu kỹ thuật, an ninh và tuân thủ các tiêu chuẩn giao thức, định dạng dữ liệu do cơ quan có thẩm quyền quy định. Dữ liệu trao đổi qua mạng phải được mã hóa và xác thực nguồn gốc, bảo đảm tính toàn vẹn và bảo mật. Hai bên kết nối phải thống nhất quy chế vận hành kết nối, bao gồm: phạm vi dữ liệu chia sẻ, tần suất hoặc thời gian thực trao đổi, trách nhiệm mỗi bên trong quản lý, sử dụng dữ liệu nhận được, và cơ chế hỗ trợ khi xảy ra sự cố kết nối.

4. Cơ quan, tổ chức ngoài Hệ thống THADS muốn khai thác dữ liệu từ Nền tảng số THADS (nếu được phép) phải được sự đồng ý bằng văn bản của Cục Quản lý THADS hoặc cơ quan có thẩm quyền. Trước khi kết nối, đơn vị kết nối phải ký kết thỏa thuận hoặc bản cam kết bảo đảm an toàn, bảo mật thông tin và dữ liệu theo quy định.

5. Dữ liệu được trao đổi, chia sẻ qua Nền tảng số THADS dưới dạng điện tử có giá trị pháp lý tương đương với tài liệu dạng giấy (nếu đáp ứng các yêu cầu theo quy định của Luật Giao dịch điện tử và pháp luật liên quan). Cơ quan, đơn vị nhận dữ liệu từ Nền tảng số THADS có trách nhiệm chấp nhận và sử dụng dữ liệu đó như tài liệu chính thức, không được đòi hỏi bản giấy nếu pháp luật không yêu cầu, đồng thời phải đảm bảo an toàn, bảo mật cho dữ liệu đã nhận theo quy định của pháp luật và Quy chế này.

6. Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS chịu trách nhiệm thiết lập, duy trì và vận hành các chức năng kỹ thuật phục vụ việc ghi nhận, lưu trữ, giám sát nhật ký truy cập, khai thác dữ liệu trên Nền tảng số THADS. Cục Quản lý THADS thực hiện kiểm tra, giám sát việc truy cập, khai thác và sử dụng dữ liệu theo thẩm quyền. Hệ thống phải lưu trữ đầy đủ nhật ký truy cập và khai thác dữ liệu để phục vụ công tác kiểm tra, giám sát, thanh tra, kiểm toán khi cần thiết, bảo đảm việc sử dụng dữ liệu đúng mục đích và đúng thẩm quyền.

Chương VI: BẢO ĐẢM AN TOÀN THÔNG TIN, BẢO MẬT DỮ LIỆU

Điều 17. Yêu cầu an toàn thông tin đối với Nền tảng số THADS

1. Nền tảng số THADS đã được xác định và phê duyệt cấp độ an toàn hệ thống thông tin (cấp độ 3) theo quy định tại Nghị định 85/2016/NĐ-CP về bảo đảm an toàn hệ thống thông tin theo cấp độ và các văn bản hướng dẫn. Trên cơ sở cấp độ được phê duyệt, Cục Quản lý THADS phối hợp với Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS triển khai đầy đủ các biện pháp bảo đảm an toàn hệ thống tương ứng với cấp độ đó; định kỳ rà soát, đánh giá lỗ hổng; diễn tập ứng cứu sự cố; kiểm tra đánh giá an toàn hệ thống hàng năm. Hệ thống phải tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin do cơ quan có thẩm quyền ban hành.

2. Toàn bộ hạ tầng mạng, máy chủ cài đặt Nền tảng số THADS cần được bảo vệ an toàn vật lý. Phòng đặt máy chủ phải đáp ứng yêu cầu kỹ thuật theo quy định pháp luật hiện hành. Định kỳ thay đổi mật khẩu quản trị các thiết bị mạng, máy chủ theo quy định về mật khẩu an toàn.

3. Ứng dụng nghiệp vụ trên Nền tảng số THADS phải được phát triển và cấu hình theo các chuẩn an toàn ứng dụng để phòng ngừa lỗ hổng. Dữ liệu trên Nền tảng số THADS được phân loại theo đặc tính của dữ liệu, gồm: dữ liệu nội bộ, dữ liệu chia sẻ giữa các cơ quan nhà nước, dữ liệu công khai và dữ liệu thuộc phạm vi bí mật nhà nước mà hệ thống được phép tiếp nhận, lưu trữ, xử lý theo quy định của pháp luật. Dữ liệu quan trọng, đặc biệt là dữ liệu cá nhân hoặc nhạy cảm, dữ liệu thuộc bí mật nhà nước phải được mã hóa khi truyền trên mạng và khi lưu trữ theo quy định. Cơ sở dữ liệu cần được phân quyền truy cập ở mức chặt chẽ nhất; chỉ các tài khoản ứng dụng và quản trị được phép truy cập trong phạm vi cần thiết. Kích hoạt cơ chế ghi nhật ký truy cập cơ sở dữ liệu để theo dõi các truy vấn bất thường. Thực hiện sao lưu cơ sở dữ liệu theo Điều 12 và lưu giữ tại khu vực an toàn.

4. Người dùng Nền tảng số THADS khi truy cập hệ thống từ máy trạm, cần tuân thủ các quy định an toàn máy trạm. Cụ thể: máy tính phải được cài phần mềm phòng chống mã độc và thường xuyên cập nhật; hệ điều hành và các ứng dụng phải cập nhật bản vá bảo mật kịp thời; không tự ý cài đặt phần mềm không được phép. Dữ liệu tải về máy trạm phải được quản lý, không lưu trên máy cá nhân.

Nếu cần sao chép dữ liệu ra thiết bị lưu trữ ngoài (USB, ổ cứng di động…), cần mã hóa tệp dữ liệu trước khi sao chép.

5. Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS cần triển khai các công cụ giám sát ATTT để phát hiện kịp thời các điểm yếu, các truy cập bất thường hoặc nguy cơ tấn công mạng trên Nền tảng số THADS. Thường xuyên kiểm tra, rà quét hệ thống để phát hiện malware, dấu hiệu bị xâm nhập. Khi phát hiện máy tính hoặc tài khoản vi phạm quy định an ninh, quản trị viên được quyền ngắt kết nối thiết bị đó ra khỏi hệ thống. Hàng tháng, đơn vị vận hành có báo cáo tổng hợp tình hình bảo đảm ATTT của hệ thống, nêu rõ các vấn đề tồn tại và kiến nghị giải pháp, gửi về Cục Quản lý THADS để theo dõi.

Điều 18. Bảo vệ dữ liệu và thông tin trên Nền tảng số THADS

1. Dữ liệu cá nhân được thu thập và xử lý trên Nền tảng số THADS phải được bảo vệ theo đúng quy định của pháp luật về bảo vệ dữ liệu cá nhân và các văn bản pháp luật có liên quan. Công chức, người lao động, cá nhân được phân công xử lý dữ liệu cá nhân có trách nhiệm không cung cấp, chia sẻ dữ liệu cá nhân cho bất kỳ tổ chức, cá nhân nào không có thẩm quyền hoặc ngoài phạm vi cho phép của pháp luật. Khi trao đổi dữ liệu cá nhân qua môi trường mạng, phải thực hiện biện pháp mã hóa hoặc sử dụng kênh truyền an toàn; trường hợp sao chép dữ liệu cá nhân ra khỏi cơ quan bằng thiết bị điện tử thì cũng phải mã hóa và áp dụng biện pháp bảo vệ phù hợp. Không sử dụng mạng xã hội, ứng dụng nhắn tin công cộng để trao đổi dữ liệu cá nhân liên quan đến thi hành án dân sự, trừ trường hợp pháp luật cho phép và bảo đảm đầy đủ biện pháp bảo mật cần thiết. Việc xóa, hủy, ẩn, ngừng xử lý hoặc tiếp tục lưu trữ dữ liệu cá nhân được thực hiện theo quy định của pháp luật về bảo vệ dữ liệu cá nhân, pháp luật về lưu trữ, pháp luật chuyên ngành và quy định về quản lý hồ sơ, tài liệu của ngành THADS.

2. Mọi thông tin, tài liệu thuộc danh mục bí mật nhà nước trong lĩnh vực thi hành án dân sự và lĩnh vực khác theo quy định phải được quản lý, lưu trữ, truyền đưa, trao đổi theo đúng quy định của pháp luật về bảo vệ bí mật nhà nước và các văn bản hướng dẫn có liên quan. Không được đưa thông tin, tài liệu bí mật nhà nước lên Nền tảng số THADS nếu Nền tảng số THADS hoặc phân hệ có liên quan chưa được cơ quan có thẩm quyền cho phép xử lý thông tin, tài liệu có độ mật tương ứng. Việc truyền đưa, trao đổi dữ liệu mật chỉ được thực hiện trên hệ thống, thiết bị chuyên dụng đã được thẩm định, đánh giá đáp ứng yêu cầu bảo mật và chỉ bởi người có thẩm quyền. Công chức khi soạn thảo, xử lý văn bản, tài liệu mật phải tuân thủ các quy định về soạn thảo, in ấn, lưu giữ, vận chuyển, sao chụp, tiêu hủy tài liệu mật theo quy định; không sao chép, tiết lộ thông tin mật cho người không có trách nhiệm; không lưu trữ thông tin mật trên thiết bị cá nhân, dịch vụ điện toán đám mây hoặc môi trường không được phép; khi phát hiện lộ, lọt thông tin mật phải báo cáo ngay cấp có thẩm quyền để xử lý.

3. Ngoài dữ liệu cá nhân và bí mật nhà nước, Nền tảng số THADS có thể chứa các thông tin nhạy cảm khác (như bí mật công tác, hồ sơ vụ việc đang điều tra, thông tin khiếu nại, tố cáo...). Những thông tin này tuy không thuộc danh mục

bí mật nhà nước nhưng cần được bảo mật theo quy định nội bộ. Người dùng và quản trị viên phải tôn trọng quyền riêng tư, bảo mật thông tin của các đối tượng liên quan; không truy cập, thu thập hoặc sử dụng các thông tin vượt quá phạm vi công việc được giao. Việc cung cấp cho bên thứ ba phải tuân thủ đúng trình tự, thủ tục pháp luật. Nếu phát hiện lỗ hổng hoặc nguy cơ mất an toàn liên quan đến dữ liệu, thông tin trên Nền tảng số THADS, phải kịp thời báo cáo để có biện pháp khắc phục.

4. Đối với Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS và cá nhân thuộc đơn vị này tham gia quản trị, vận hành, bảo trì hệ thống, trước khi tiếp cận hệ thống, dữ liệu hoặc môi trường vận hành của Nền tảng số THADS, phải thực hiện ký cam kết bảo mật thông tin theo quy định. Trường hợp sử dụng mã nguồn, hạ tầng hoặc dịch vụ của bên thứ ba để phục vụ việc triển khai, vận hành Nền tảng số THADS, thì phải bảo đảm bên thứ ba đó đáp ứng các yêu cầu tương đương về bảo mật, an toàn thông tin, bảo vệ dữ liệu cá nhân và bảo vệ bí mật nhà nước theo quy định tại Quy chế này và các quy định pháp luật có liên quan.

Chương VII: TỔ CHỨC THỰC HIỆN

Điều 19. Trách nhiệm của Cục Công nghệ thông tin

1. Chủ trì duy trì, bảo đảm hạ tầng kỹ thuật, hạ tầng kết nối, chia sẻ dữ liệu phục vụ việc triển khai, vận hành kết nối Nền tảng số THADS trong phạm vi chức năng, nhiệm vụ được giao; bảo đảm hệ thống hoạt động ổn định, thông suốt, đáp ứng yêu cầu kết nối liên thông trong và ngoài Bộ Tư pháp.

2. Phối hợp với Cục Quản lý THADS và Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS trong việc bảo đảm an toàn thông tin mạng đối với Nền tảng số THADS; tham gia kiểm tra, đánh giá định kỳ hoặc đột xuất về an toàn, an ninh thông tin theo quy định.

3. Hướng dẫn về tiêu chuẩn, quy chuẩn kỹ thuật, giải pháp công nghệ, mô hình kiến trúc và các yêu cầu kỹ thuật khác nhằm bảo đảm Nền tảng số THADS phù hợp với Khung kiến trúc Chính phủ điện tử/Chính phủ số của Bộ Tư pháp và quy định của pháp luật có liên quan.

4. Phối hợp xử lý sự cố kỹ thuật nghiêm trọng liên quan đến hạ tầng, kết nối, an toàn thông tin; tham gia đề xuất phương án khắc phục, phòng ngừa rủi ro, bảo đảm duy trì hoạt động liên tục của hệ thống.

Điều 20. Trách nhiệm của Cục Quản lý THADS

1. Cục Quản lý THADS là đơn vị đầu mối tổ chức quản lý, vận hành tập trung Nền tảng số THADS; thực hiện quản lý tài khoản quản trị cấp Cục; chủ trì, phối hợp với Cục Công nghệ thông tin và Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS trong việc duy trì hệ thống hoạt động ổn định, an toàn, bảo đảm chất lượng dịch vụ theo quy định. Trường hợp có nguy cơ không bảo đảm

các chỉ tiêu chất lượng dịch vụ, Cục Quản lý THADS có trách nhiệm yêu cầu Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS đề xuất biện pháp khắc phục, đồng thời tổ chức theo dõi, giám sát việc thực hiện các biện pháp đó. Cục Quản lý THADS chịu trách nhiệm trước Lãnh đạo Bộ về hiệu quả khai thác, sử dụng Nền tảng số THADS.

2. Ban hành và hướng dẫn thực hiện các quy chế, quy định, văn bản chỉ đạo liên quan đến Nền tảng số THADS; định kỳ rà soát, đề xuất sửa đổi, bổ sung phù hợp với quy định pháp luật và yêu cầu thực tiễn.

Tổ chức quản lý vận hành tập trung; quản lý tài khoản quản trị cấp Cục; phối hợp với Cục Công nghệ thông tin và Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS bảo đảm hệ thống hoạt động ổn định, an toàn.

3. Thiết lập đầu mối hỗ trợ kỹ thuật, nghiệp vụ; tổ chức tập huấn, bồi dưỡng, hướng dẫn các Cơ quan THADS địa phương trong quá trình triển khai, sử dụng hệ thống.

4. Tổ chức kiểm tra, giám sát việc chấp hành Quy chế; yêu cầu báo cáo định kỳ hoặc đột xuất; tổng hợp, đánh giá tình hình sử dụng Nền tảng số THADS trong toàn hệ thống.

5. Chủ trì đề xuất nâng cấp, điều chỉnh, hoàn thiện các chức năng nghiệp vụ của Nền tảng số THADS đáp ứng yêu cầu thực tiễn; tổ chức quản lý, giám sát việc thực hiện hợp đồng cung cấp dịch vụ liên quan đến Nền tảng số THADS, bảo đảm Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS tuân thủ các cam kết về chất lượng dịch vụ, mức độ đáp ứng dịch vụ, yêu cầu bảo mật, nghĩa vụ hỗ trợ kỹ thuật, cung cấp tài liệu kỹ thuật, tham gia đào tạo, hướng dẫn sử dụng theo yêu cầu; kịp thời yêu cầu khắc phục và tham mưu, đề xuất biện pháp xử lý theo quy định của hợp đồng và pháp luật có liên quan trong trường hợp phát hiện vi phạm hoặc có nguy cơ không đáp ứng các cam kết đã thỏa thuận.

Điều 21. Trách nhiệm của các Cơ quan THADS địa phương

1. Cơ quan THADS địa phương có trách nhiệm triển khai ứng dụng, vận hành và khai thác Nền tảng số THADS tại đơn vị mình, bảo đảm hệ thống hoạt động an toàn, hiệu quả, phục vụ yêu cầu nghiệp vụ. Thủ trưởng Cơ quan THADS địa phương có trách nhiệm quán triệt Quy chế này đến toàn thể công chức, người lao động thuộc phạm vi quản lý; tổ chức phân công nhiệm vụ rõ ràng trong việc quản lý, vận hành và sử dụng Nền tảng số THADS.

2. Mỗi Cơ quan THADS địa phương cần phân công một đầu mối phụ trách CNTT để quản trị, hỗ trợ kỹ thuật vận hành tại địa phương và làm đầu mối liên hệ với Cục Quản lý THADS. Đảm bảo bố trí đủ nhân sự có năng lực để thực hiện các nhiệm vụ: quản lý tài khoản người dùng của địa phương, hỗ trợ nghiệp vụ cho cán bộ trong sử dụng Nền tảng số THADS, phối hợp xử lý sự cố với đơn vị vận hành… Đồng thời, đơn vị phải bố trí các nguồn lực cần thiết (trang thiết bị, kinh phí vận hành trong phạm vi được giao) để duy trì hoạt động của Nền tảng số THADS tại đơn vị.

3. Cơ quan THADS địa phương có trách nhiệm tuân thủ nghiêm các quy định về CNTT, ATTT và các nội dung của Quy chế này trong quá trình sử dụng Nền tảng số THADS. Thủ trưởng đơn vị chịu trách nhiệm kiểm tra, giám sát việc chấp hành của công chức thuộc thẩm quyền quản lý, kịp thời chỉ đạo và có biện pháp ngăn chặn hành vi vi phạm (nếu có). Mỗi cán bộ sử dụng Nền tảng số THADS phải nêu cao ý thức bảo vệ dữ liệu, bảo mật tài khoản.

4. Khi xảy ra sự cố hoặc vấn đề bất thường liên quan đến Nền tảng số THADS tại đơn vị, Cơ quan THADS địa phương có trách nhiệm chủ động xử lý trong phạm vi khả năng (nếu là vấn đề đơn giản) và đồng thời báo cáo ngay về Cục Quản lý THADS (hoặc đầu mối hỗ trợ kỹ thuật) để được hướng dẫn giải quyết tiếp. Phối hợp chặt chẽ với Đơn vị vận hành kỹ thuật Nền tảng số trong lĩnh vực THADS và Cục Quản lý THADS trong quá trình khắc phục sự cố, đảm bảo thông tin thông suốt.

5. Đề xuất những sáng kiến, giải pháp cải tiến Nền tảng số THADS hoặc góp ý sửa đổi Quy chế (khi cần) nhằm nâng cao hiệu quả ứng dụng công nghệ thông tin, chuyển đổi số trong lĩnh vực thi hành án dân sự.

Điều 22. Tổ chức thực hiện

1. Cục Quản lý THADS có trách nhiệm tổ chức triển khai, hướng dẫn thực hiện Quy chế đến từng đơn vị trong hệ thống, Thủ trưởng các đơn vị thuộc Cục, cơ quan, đơn vị liên quan có trách nhiệm phổ biến, quán triệt Quy chế tới toàn thể công chức, viên chức, người lao động thuộc phạm vi quản lý.

2. Những nội dung về quản lý, vận hành, khai thác, sử dụng Nền tảng số THADS chưa được quy định tại Quy chế này hoặc được quy định tại Quy chế này nhưng có sự thay đổi do văn bản quy phạm pháp luật mới ban hành thì thực hiện theo quy định của pháp luật hiện hành có liên quan, bao gồm pháp luật về thi hành án dân sự, công nghệ thông tin, giao dịch điện tử, lưu trữ, an toàn thông tin mạng, an ninh mạng, bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân và các quy định pháp luật khác có liên quan./.