BỘ TƯ PHÁP
CỤC TRỢ GIÚP PHÁP LÝ

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

Số: 76 /QĐ-TGPL

Hà Nội, ngày 25 tháng 11 năm 2022

QUYẾT ĐỊNH
Ban hành Nội quy đảm bảo an ninh mạng của Cục Trợ giúp pháp lý

CỤC TRƯỞNG CỤC TRỢ GIÚP PHÁP LÝ

Căn cứ Luật An ninh mạng năm 2018;

Căn cứ Luật Bảo vệ bí mật nhà nước năm 2018;

Căn cứ Luật giao dịch điện tử năm 2005;

Căn cứ Nghị định số 130/2018/NĐ-CP ngày 27/9/2018 của Chính phủ quy định chi tiết thi hành Luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số;

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

Căn cứ Nghị định số 96/2017/NĐ-CP ngày 16/8/2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Tư pháp;

Căn cứ Quyết định số 768/QĐ-BTP ngày 18/4/2018 của Bộ Tư pháp quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Cục Trợ giúp pháp lý.

Theo đề nghị của Trung tâm Thông tin, dữ liệu trợ giúp pháp lý và Văn phòng Cục.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Nội quy đảm bảo an ninh mạng của Cục Trợ giúp pháp lý".

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

Điều 3. Trưởng các đơn vị thuộc Cục, công chức, viên chức, người lao động của Cục Trợ giúp pháp lý có trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3 (để thực hiện);
- Thứ trưởng Mai Lương Khôi (để báo cáo);
- Văn phòng Bộ, Cục Công nghệ thông tin (để phối hợp);
- Lưu: VT, TTTTDL.

CỤC TRƯỞNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
CỤC TRỢ GIÚP PHÁP LÝ
BỘ TƯ PHÁP

Cù Thu Anh

NỘI QUY

Đảm bảo an ninh mạng của Cục Trợ giúp pháp lý

(Ban hành kèm theo Quyết định số 76/QĐ-TGPL ngày 25 tháng 11 năm 2022 của Cục trưởng Cục Trợ giúp pháp lý)

Chương I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

1. Phạm vi điều chỉnh: Nội quy này quy định về đảm bảo an ninh mạng trong các hoạt động của Cục Trợ giúp pháp lý.

2. Đối tượng áp dụng: Nội quy đảm bảo an ninh mạng của Cục Trợ giúp pháp lý áp dụng đối với các đơn vị thuộc Cục, công chức, viên chức, người lao động thuộc Cục.

Điều 2. Nguyên tắc bảo vệ an ninh mạng trong hoạt động của Cục

1. Tuân thủ nghiêm các quy định của Luật An ninh mạng (ANM), các văn bản hướng dẫn thi hành Luật và quy định của Bộ Tư pháp.

2. Kết hợp chặt chẽ giữa nhiệm vụ bảo vệ ANM với công tác bảo vệ bí mật nhà nước (BMNN) tại Cục.

3. Thực hiện các biện pháp bảo vệ ANM phù hợp với chức năng, nhiệm vụ và điều kiện thực tiễn về cơ sở vật chất của Cục.

Điều 3. Hành vi bị cấm trong công tác an ninh mạng tại Cục

1. Các hành vi đã được quy định tại Điều 8 Luật An ninh mạng.

2. Sử dụng các trang thiết bị có kết nối mạng internet, mạng nội bộ, mạng viễn thông và các phương thức khác để tạo lập, sao chụp, truyền tải, lưu trữ thông tin chứa BMNN.

3. Truy cập không đúng thẩm quyền vào cơ sở dữ liệu các hệ thống thông tin quản lý phục vụ công tác chỉ đạo, điều hành, thống kê, báo cáo và các phần mềm tiện ích khác; truy cập các website có tiềm ẩn nguy cơ gây mất an toàn, an ninh mạng.

4. Sử dụng các thiết bị, phương tiện lưu trữ, truyền tải thông tin (không đúng quy định) như: usb, ổ cứng di động… để sao chép thông tin từ máy tính soạn thảo văn bản mật.

Chương II

NHỮNG QUY ĐỊNH CỤ THỂ

Điều 4. Quy định sử dụng máy tính, máy in tại Cục

1. Toàn bộ máy tính phải được cài đặt mật khẩu, khóa máy hoặc tắt máy khi ngừng sử dụng.

2. Máy tính phải được cài đặt các phần mềm hợp lệ (các phần mềm, hệ điều hành phù hợp, phần mềm phòng chống virus ...). Khi phát hiện máy tính có dấu hiệu bị mất an toàn, an ninh thông tin hoặc bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm phần mềm độc hại, người sử dụng phải tắt máy và báo cho Cục Công nghệ thông tin để được kiểm tra, xử lý kịp thời.

3. Người sử dụng chỉ truy nhập vào các Trang/Cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và khai thác các thông tin phù hợp với chức năng, nhiệm vụ, quyền hạn của mình; có trách nhiệm bảo mật tài khoản.

4. Khi thay thế máy tính, công chức, viên chức và người lao động phối hợp với Văn phòng Cục để thực hiện xóa toàn bộ dữ liệu trên máy tính cũ trước khi chuyển giao về Văn phòng Cục. Việc chuyển giao phải được lập biên bản và ký xác nhận giữa các bên.

5. Đối với máy tính, máy in phục vụ soạn thảo và in tài liệu mật và máy hủy tài liệu mật (gọi tắt là máy tính mật, máy in mật và máy hủy mật):

a) Về trang bị máy tính mật, máy in mật và máy hủy mật:

Cục bố trí 03 (ba) bộ máy tính, máy in và máy hủy đặt tại Văn phòng Cục, Phòng Chính sách và Quản lý nghiệp vụ trợ giúp pháp lý và Phòng Tài chính và Quản lý chất lượng trợ giúp pháp lý để phục vụ các công chức, viên chức soạn thảo, in và hủy tài liệu mật.

Máy tính mật phải kết nối với máy in mật và các thiết bị này không được kết nối internet, mạng nội bộ, mạng viễn thông.

b) Các đơn vị thuộc Cục được giao các trang thiết bị có trách nhiệm bảo quản an toàn đối với máy tính mật, máy in mật và máy hủy mật; chỉ công chức, viên chức và người lao động có trách nhiệm soạn thảo, in tài liệu mật mới được sử dụng máy tính mật, máy in tài liệu mật. Khi có nhu cầu soạn thảo, in tài liệu mật, hủy tài liệu mật, công chức, viên chức và người lao động có trách nhiệm thông báo và đăng ký sử dụng với đơn vị quản lý, ghi sổ theo dõi sử dụng máy tính mật, máy in mật, máy hủy mật; file văn bản phải được đặt mật khẩu riêng. Sau khi sử dụng xong, công chức, viên chức và người lao động soạn thảo văn bản mật phải tắt máy tính mật, máy in mật và thông báo cho đơn vị quản lý để bảo quản an toàn máy tính mật, máy in mật, máy hủy mật.

Điều 5. Quy định về sử dụng mạng Internet

Công chức, viên chức và người lao động trong đơn vị chỉ truy cập mạng Internet để thu thập, khai thác, tham khảo thông tin, dữ liệu phục vụ công tác nghiên cứu, học tập, thực thi hiệu quả hơn nhiệm vụ chuyên môn được giao.

Điều 6. Các hoạt động đảm bảo an ninh mạng

1. Triển khai thực hiện các quy định tại Chương IV Luật An ninh mạng có liên quan đến chức năng, nhiệm vụ của Cục.

2. Đảm bảo an ninh mạng đối với Trang/Cổng thông tin điện tử trợ giúp pháp lý Việt Nam và các hệ thống thông tin quản lý, phần mềm tiện ích khác do Cục Trợ giúp pháp lý quản lý.

a) Khi phát hiện bất kỳ dấu hiệu nào liên quan đến các hoạt động xâm nhập bất hợp pháp hoặc nguy cơ khác đe dọa an ninh mạng đối với Cổng/Trang thông tin điện tử trợ giúp pháp lý Việt Nam và các hệ thống thông tin quản lý, phần mềm tiện ích khác do Cục Trợ giúp pháp lý quản lý, Cục Trợ giúp pháp lý phải báo Cục Công nghệ thông tin để được kiểm tra, xử lý kịp thời.

b) Triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn hành vi gián điệp mạng, xâm phạm bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin và kịp thời gỡ bỏ thông tin liên quan đến hành vi này.

c) Trong trường hợp cần thiết phối hợp, thực hiện yêu cầu của lực lượng chuyên trách an ninh mạng về phòng, chống gián điệp mạng, bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên hệ thống thông tin.

3. Quản lý tài khoản truy cập

a) Cá nhân sử dụng, truy cập các hệ thống thông tin quản lý, phần mềm tiện ích do Cục Trợ giúp pháp lý quản lý được cấp tài khoản và có trách nhiệm bảo quản tài khoản được cấp.

b) Trường hợp cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu, trong vòng không quá **5** ngày làm việc cơ quan, đơn vị quản lý cá nhân đó phải thông báo cơ quan, đơn vị chủ quản các hệ thống thông tin quản lý, phần mềm tiện ích của Cục Trợ giúp pháp lý để điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng đối với các hệ thống thông tin quản lý, phần mềm tiện ích của Cục Trợ giúp pháp lý.

c) Cục Trợ giúp pháp lý có quyền khóa/xóa tài khoản trong trường hợp phát hiện tài khoản có các hành vi tấn công hoặc để xảy ra vấn đề mất an toàn, an ninh thông tin trong quá trình vận hành, khai thác các hệ thống thông tin quản lý, phần mềm tiện ích do Cục Trợ giúp pháp lý quản lý.

4. Đảm bảo an ninh mạng thông tin, dữ liệu công vụ

a) Thực hiện bảo vệ thông tin, dữ liệu liên quan đến hoạt động công vụ, thông tin có nội dung quan trọng hoặc không phải là thông tin công khai bằng các biện pháp như: thiết lập phương án đảm bảo tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu; mã hóa thông tin, dữ liệu khi lưu trữ trên hệ thống/thiết bị lưu trữ dữ liệu di động; sử dụng chữ ký số để xác thực và bảo mật thông tin, dữ liệu.

b) Có phương thức để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin để dễ dàng theo dõi và quản lý, khai thác.

c) Các đơn vị thuộc Cục và công chức, viên chức, người lao động thuộc Cục phải thường xuyên kiểm tra, giám sát các hoạt động chia sẻ, gửi, nhận thông tin, dữ liệu trong hoạt động nội bộ của mình; khuyến cáo việc chia sẻ, gửi, nhận thông tin trên môi trường mạng cần phải sử dụng mật khẩu để bảo vệ thông tin.

d) Đối với hoạt động trao đổi thông tin, dữ liệu với bên ngoài, các đơn vị thuộc Cục và từng cá nhân thực hiện trao đổi thông tin, dữ liệu ra bên ngoài cam kết và có biện pháp bảo mật thông tin, dữ liệu được trao đổi. Giao dịch trực tuyến phải được truyền đầy đủ, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép; sử dụng các cơ chế xác thực mạnh, chữ ký số khi tham gia giao dịch, sử dụng các giao thức truyền thông an toàn.

Chương III
TỔ CHỨC THỰC HIỆN

Điều 7. Trách nhiệm của Trung tâm Thông tin, dữ liệu trợ giúp pháp lý

1. Là đầu mối trong các hoạt động chuyên môn và phối hợp với các đơn vị liên quan về đảm bảo an ninh mạng.

2. Tham mưu giúp Cục trưởng Cục Trợ giúp pháp lý triển khai, hướng dẫn, đôn đốc, kiểm tra, theo dõi việc thực hiện các quy định bảo vệ ANM trong công tác của Cục và nội quy này tại Cục; đề xuất Cục trưởng các biện pháp, trang thiết bị để bảo vệ ANM tại Cục.

3. Thực hiện các công việc khác được giao liên quan đến đảm bảo an ninh mạng của Cục Trợ giúp pháp lý.

Điều 8. Trách nhiệm của Trưởng các đơn vị thuộc Cục

Trưởng các đơn vị thuộc Cục chịu trách nhiệm trước Cục trưởng trong việc tổ chức thực hiện các quy định bảo vệ ANM đối với những nội dung thuộc phạm vi chức năng, nhiệm vụ của đơn vị và những nội dung được Cục trưởng phân công thực hiện.

Trưởng các đơn vị thuộc Cục có trách nhiệm tuyên truyền phổ biến, quán triệt, tổ chức đào tạo tập huấn cho công chức, viên chức và người lao động trong đơn vị tuân thủ các quy định của pháp luật về công tác đảm bảo an toàn thông tin, an ninh mạng.

Điều 9. Trách nhiệm của công chức, viên chức và người lao động thuộc Cục

1. Tuân thủ các quy định của pháp luật, của Bộ Tư pháp, Nội quy của Cục về bảo vệ an ninh mạng trong quá trình thực thi công vụ.

2. Chủ động, kịp thời báo cáo với lãnh đạo đơn vị và phối hợp chặt chẽ với Văn phòng Cục để khắc phục tình trạng hỏng hóc của các trang thiết bị được giao để thực thi công vụ.

3. Khi chuyển công tác, nghỉ việc, nghỉ chế độ phải bàn giao các trang thiết bị kèm toàn bộ thông tin, tư liệu được tạo lập, lưu trữ trên thiết bị đó theo chức năng, nhiệm vụ được giao. Không tự ý xóa bỏ thông tin, tư liệu liên quan đến việc thực thi công vụ trên các trang thiết bị.

Trong quá trình triển khai thực hiện Nội quy này, nếu phát sinh vướng mắc, các đơn vị, cá nhân thuộc Cục kịp thời phản ánh về Trung tâm Thông tin, dữ liệu trợ giúp pháp lý để được hướng dẫn hoặc báo cáo Cục trưởng xem xét, quyết định./.