BỘ TƯ PHÁP
TRƯỜNG ĐẠI HỌC LUẬT HÀ NỘI

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Số: 2581 /QĐ-ĐHLHN

Hà Nội, ngày 05 tháng 7 năm 2022

QUYẾT ĐỊNH
Về việc ban hành Quy chế Hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng tại Trường Đại học Luật Hà Nội

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

Căn cứ Luật Viễn thông ngày 23 tháng 11 năm 2009;

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

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

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Nghị định 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 03/2013/TT-BTTTT ngày 22 tháng 01 năm 2013 của Bộ trưởng Bộ Thông tin và Truyền thông quy định áp dụng tiêu chuẩn, quy chuẩn kỹ thuật đối với Trung tâm dữ liệu;

Căn cứ Quyết định số 405/CP ngày 10/11/1979 của Hội đồng Chính phủ về việc thành lập Trường Đại học Pháp lý Hà Nội (nay là Trường Đại học Luật Hà Nội);

Căn cứ Quyết định số 868/QĐ-BTP ngày 07/5/2015 của Bộ trưởng Bộ Tư pháp quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Trường Đại học Luật Hà Nội;

Căn cứ Nghị quyết số 3776/NQ-HĐTĐHLHN ngày 23 tháng 10 năm 2020 của Hội đồng trường Trường Đại học Luật Hà Nội ban hành Quy chế tổ chức và hoạt động của Trường Đại học Luật Hà Nội;

Xét đề nghị của Giám đốc Trung tâm Công nghệ thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy chế Hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng tại Trường Đại học Luật Hà Nội".

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

Điều 3. Giám đốc Trung tâm Công nghệ thông tin, lãnh đạo các đơn vị, và các tổ chức, cá nhân liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Hội đồng Trường (để chỉ đạo t/h)
- Các Phó Hiệu trưởng (để chỉ đạo t/h);
- Trưởng các đơn vị (để t/h);
- Lưu VT, TTCNTT.

HIỆU TRƯỞNG

BỘ TƯ PHÁP TRƯỜNG ĐẠI HỌC LUẬT HÀ NỘI

Đoàn Trung Kiên

BỘ TƯ PHÁP
TRƯỜNG ĐẠI HỌC LUẬT HÀ NỘI

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

QUY CHẾ
Hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng tại Trường Đại học Luật Hà Nội

(Ban hành kèm theo Quyết định số 2581/QĐ/ĐHLHN ngày 05 tháng 7 năm 2022 của Hiệu trưởng Trường Đại học Luật Hà Nội)

CHƯƠNG I
QUY ĐỊNH CHUNG

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

1. Quy chế này quy định về nhiệm vụ, quyền hạn, trách nhiệm, nguyên tắc và chế độ hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng *(viết tắt là ƯCSCATTTM)* Trường Đại học Luật Hà Nội.

2. Quy chế này áp dụng cho các thành viên Đội ƯCSCATTTM thuộc Trung tâm Công nghệ thông tin *(viết tắt là CNTT)* Trường Đại học Luật Hà Nội; các đơn vị, tổ chức, cá nhân có liên quan tới hoạt động ƯCSCATTTM tại Trường Đại học Luật Hà Nội.

Điều 2. Giải thích từ ngữ

1. Sự cố an toàn thông tin mạng là việc thông tin, hệ thống thông tin bị tấn công hoặc gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng của thông tin, hệ thống thông tin.

2. Sự cố an toàn thông tin mạng nghiêm trọng là sự cố có một hoặc nhiều tính chất sau: Có khả năng xảy ra trên diện rộng, thời gian xảy ra nhanh; có khả năng phá hoại hệ thống mạng máy tính; hệ thống bị mất quyền điều khiển; lấy cắp dữ liệu, có thể gây thiệt hại lớn cho các hệ thống thông tin trên mạng, các hệ thống thông tin quan trọng của Trường.

3. Ứng cứu sự cố an toàn thông tin mạng là hoạt động nhằm xử lý, khắc phục sự cố gây mất an toàn thông tin mạng gồm theo dõi,thu thập, phân tích, phát hiện, cảnh báo, kiểm tra, xác minh sự cố, ngăn chặn sự cố, khôi phục dữ liệu và khôi phục hoạt động bình thường của hệ thống thông tin.

4. Log file là tập tin được tạo ra trong quá trình hoạt động của thiết bị công nghệ thông tin

Điều 3. Tổ chức Đội ứng cứu sự cố an toàn thông tin mạng

1. Đội ƯCSCATTTM gồm các thành viên là viên chức, người lao động thuộc Trung tâm Công nghệ thông tin chuyên trách về quản trị mạng và hạ tầng CNTT Trường Đại học Luật Hà Nội. Đội trưởng là Giám đốc Trung tâm và đội

phó là Phó Giám đốc Trung tâm.

2. Đội ƯCSCATTTM có thông tin liên hệ như sau:

- Số điện thoại thường trực: (0243) 7733287;
- Hộp thư điện tử của Đội ƯCSCATTTM: trungtam_cntt@hlu.edu.vn

Điều 4. Nhiệm vụ và quyền hạn của Đội ứng cứu sự cố an toàn thông tin mạng

1. Là đầu mối của Trường để tham gia hoạt động ƯCSCATTTM toàn Trường. Có trách nhiệm liên kết, phối hợp với các đơn vị trong Trường về ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng để thu thập thông tin, kịp thời cảnh báo sự cố và các điểm yếu, lỗ hổng bảo mật, các nguồn tấn công máy tính nhằm giúp các cơ quan, đơn vị chủ động phòng chống, giảm thiểu rủi ro, mất an toàn thông tin mạng.

2. Hỗ trợ đơn vị trong Trường trong công tác đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin (CNTT) và tổ chức hoạt động ƯCSCATTTM trong các đơn vị.

3. Được quyền truy cập vào hệ thống mạng, hệ thống ứng dụng CNTT, cơ sở dữ liệu, log file của các đơn vị để phân tích, truy vết,thực hiện dưới sự giám sát của đơn vị bị sự cố mất an toàn thông tin mạng.

CHƯƠNG II
NGUYÊN TẮC, CHẾ ĐỘ LÀM VIỆC VÀ KINH PHÍ HOẠT ĐỘNG

Điều 5. Nguyên tắc hoạt động

1. Đội ƯCSCATTTM hoạt động theo nguyên tắc tập thể lãnh đạo, cá nhân phụ trách; Đội ƯCSCATTTM chịu trách nhiệm tổ chức triển khai, kiểm tra, theo dõi, tổng hợp đánh giá tình hình và kết quả thực hiện nhiệm vụ của Đội ƯCSCATTTM.

2. Tổ chức ƯCSCATTTM phải đúng quy trình ứng cứu sự cố dựa trên tính chất, mức độ, phạm vi và nguyên nhân xảy ra sự cố theo quy định tại Thông tư số 20/2017/TT-BTTTT, Quyết định số 05/2017/QĐ-TTg; và các quy định pháp luật khác bảo đảm nhanh chóng, chính xác, kịp thời, hiệu quả và an toàn thông tin.

3. Thông tin được trao đổi, cung cấp trong quá trình điều phối, xử lý sự cố phải được bảo đảm bí mật theo yêu cầu của cơ quan, đơn vị gặp sự cố trừ khi sự cố xảy ra có liên quan tới nhiều đối tượng khác mà cần cảnh báo, nhắc nhở.

Điều 6. Chế độ làm việc

1. Các thành viên làm việc theo chế độ kiêm nhiệm và được hưởng các chế độ theo quy định hiện hành.

2. Khi có sự cố đột xuất mất an toàn thông tin xảy ra, Đội trưởng sẽ thông

báo triệu tập và điều phối các thành viên, hoặc ủy quyền cho 01 Đội phó thực hiện thẩm quyền của mình khi vắng mặt. Đội phó được ủy quyền, được sử dụng thẩm quyền của Đội trưởng để điều phối các hoạt động và chịu trách nhiệm về các quyết định của mình trước Đội trưởng và trước pháp luật. Các thành viên phải nghiêm túc thực hiện theo sự điều phối của Đội trưởng và Đội phó được ủy quyền.

Điều 7. Điều kiện và kinh phí hoạt động

1. Đội ƯCSCATTTM được đảm bảo phương tiện, thiết bị và điều kiện cần thiết để duy trì hoạt động.

2. Kinh phí hoạt động của Đội ƯCSCATTTM từ ngân sách Trường và theo Quy chế chi tiêu nội bộ của Trường Đại học Luật Hà Nội.

CHƯƠNG III
TỔ CHỨC ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN MẠNG

Điều 8. Tiếp nhận và xử lý sự cố

1. Thường trực Đội ƯCSCATTTM tiếp nhận được thông báo sự cố phải báo cáo ngay cho Đội trưởng. Nội dung tiếp nhận bao gồm:

a) Tên, địa chỉ Đơn vị vận hành hệ thống thông tin; hệ thống thông tin bị sự cố; thời điểm phát hiện sự cố;

b) Đầu mối liên lạc về sự cố của đơn vị vận hành hệ thống bị sự cố: Tên, chức vụ, điện thoại, thư điện tử;

c) Mô tả về sự cố: Loại sự cố, hiện tượng, đánh giá sơ bộ mức độ nguy hại, mức độ lây lan, tác động của sự cố đến hoạt động bình thường của tổ chức;

d) Đơn vị cung cấp dịch vụ hạ tầng công nghệ thông tin, viễn thông;

đ) Liệt kê các biện pháp đã triển khai hoặc dự kiến triển khai để xử lý khắc phục sự cố;

e) Các tổ chức, doanh nghiệp đang hỗ trợ ứng cứu, xử lý và kết quả xử lý sự cố tính đến thời điểm báo cáo;

g) Kết quả ứng cứu sự cố ban đầu;

h) Kiến nghị đề xuất hướng ứng cứu xử lý sự cố (nếu có);

i) Thông tin khác theo yêu cầu của Thường trực Đội ƯCSCATTTM.

2. Đội trưởng đưa ra yêu cầu điều phối tới các thành viên trong Đội; triệu tập cuộc họp; huy động các nguồn lực hỗ trợ khi cần thiết.

3. Khi các thành viên Đội ƯCSCATTTM nhận được thông báo điều phối phải thực hiện:

a) Tập hợp đúng thời gian, địa điểm theo sự điều phối của Thường trực Đội ƯCSCATTTM để tổ chức ứng cứu sự cố.

b) Xử lý sự cố theo sự phân công của Đội trưởng.

c) Báo cáo sự cố cho Thường trực Đội ƯCSCATTTM trong trường hợp không xử lý được.

Điều 9. Điều phối ứng cứu sự cố

1. Quy trình điều phối ƯCSCATTTM phải tuân thủ theo quy trình tổng thể phương án ƯCSCATTTM quy định tại Quyết định 05/2017/QĐ-TTg ngày 16/03/2017 của Chính phủ về việc quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia, và các quy định pháp luật khác.

2. Thường trực Đội ƯCSCATTTM thực hiện việc triệu tập, điều phối bằng văn bản đối với các thành viên trong Đội ƯCSCATTTM. Trong trường hợp khẩn cấp có thể thông báo bằng điện thoại, email để điều phối và có thông báo bằng văn bản sau. Thường trực Đội ƯCSCATTTM thông báo cho các tổ chức, cá nhân gặp sự cố về yêu cầu phối hợp trong quá trình thực hiện điều phối và ứng cứu sự cố.

3. Thành viên Đội ƯCSCATTTM tiếp nhận yêu cầu điều phối; phối hợp chặt chẽ với đơn vị nơi xảy ra sự cố và các thành viên cùng tham gia ứng cứu tổ chức thực hiện hoạt động ứng cứu theo đúng yêu cầu điều phối; báo cáo, phản hồi đầy đủ kết quả thực hiện cho Thường trực Đội ƯCSCATTTM.

4. Sau khi khắc phục sự cố, thành viên mạng lưới tham gia ứng cứu phải có trách nhiệm:

a) Rà soát, xác định nguyên nhân cơ bản gây ra sự cố;

b) Tổ chức kiểm tra lại và khắc phục triệt để sự cố;

c) Bảo đảm hệ thống hoạt động bình thường trước khi bàn giao toàn bộ hệ thống cho cơ quan, đơn vị chủ quản.

5. Thường trực Đội ƯCSCATTTM phải lưu trữ thông báo sự cố và biên bản xử lý sự cố; lưu trữ yêu cầu điều phối và báo cáo kết quả thực hiện yêu cầu điều phối trong thời gian tối thiểu 02 năm, bao gồm các thông tin sau:

a) Nội dung thông báo sự cố, thời gian tiếp nhận thông báo, thời gian gửi xác nhận;

b) Kết quả xử lý sự cố, nguyên nhân gây ra sự cố, thời gian xử lý sự cố và danh sách các tổ chức, cá nhân cùng tham gia phối hợp xử lý sự cố (nếu có).

Điều 10. Quy trình ứng cứu sự cố an toàn thông tin mạng

1. Đối với sự cố an toàn thông tin mạng thực hiện quy trình ƯCSCATTTM theo Thông tư số 20/2017/TT-BTTTT.

2. Đối với sự cố an toàn thông tin mạng nghiêm trọng thực hiện quy trình ứng cứu sự cố theo Điều 14 Quyết định số 05/2017/QĐ-TTg.

3. Quy trình ƯCSCATTTM phải thực hiện đồng thời với các văn bản hướng dẫn, quy định khác có liên quan của Bộ Thông tin và Truyền thông và Cơ

quan điều phối quốc gia.

CHƯƠNG IV
TRÁCH NHIỆM CỦA TỔ CHỨC, CÁ NHÂN

Điều 11. Thường trực Đội ứng cứu sự cố an toàn thông tin mạng

1. Chủ trì, phối hợp với các thành viên xây dựng kế hoạch, kinh phí hoạt động của Đội; triển khai công tác đảm bảo an toàn thông tin hàng năm.

2. Thường trực Đội ƯCSCATTTM thực hiện chức năng điều phối các hoạt động ứng cứu sự cố tại Trường Đại học Luật Hà Nội và có quyền điều động các thành viên trong ĐộiƯCSCATTTM phối hợp ngăn chặn, xử lý và khắc phục sự cố mạng máy tính.

3. Là đầu mối liên lạc, tiếp nhận thông tin, các phản ánh sự cố; giúp Đội trưởng điều phối ứng cứu sự cố tại Trường.

4. Tham mưu xây dựng, áp dụng quy trình, phương án ƯCSCATTTM của Trường.

5. Tổ chức các hoạt động thông tin tuyên truyền, hướng dẫn chính sách, quy định của pháp luật, nâng cao nhận thức về an toàn thông tin mạng đối với các đơn vị, tổ chức, cá nhân tại Trường và các hoạt động khác liên quan đến điều phối và ứng cứu sự cố.

Điều 12. Bộ phận giúp việc Đội ứng cứu sự cố an toàn thông tin mạng

1. Là đầu mối liên lạc, tiếp nhận, điều phối xử lý sự cố từ Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT); tham gia các hoạt động của mạng lưới ứng cứu sự cố ATTT mạng quốc gia; phát hiện và xử lý các sự cố mạng, máy tính tại trường; đảm bảo liên lạc thông suốt liên tục 24h/ngày và 7 ngày/tuần.

2. Tham mưu đề xuất các phương tiện, điều kiện đảm bảo sẵn sàng đối phó, ứng cứu, khắc phục sự cố:

- Tham mưu mua sắm, nâng cấp, gia hạn bản quyền trang thiết bị, phần mềm, công cụ, phương tiện phục vụ ứng cứu, khắc phục sự cố.

- Chuẩn bị các điều kiện bảo đảm, dự phòng nhân lực, vật lực, để sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra.

- Tổ chức, triển khai các hoạt động theo kế hoạch của Đội ƯCSCATTTM, bộ phận tác nghiệp ứng cứu sự cố; thuê dịch vụ kỹ thuật và tổ chức, duy trì đội chuyên gia ƯCSCATTTM.

3. Tham mưu triển khai các chương trình huấn luyện, diễn tập và phòng ngừa sự cố và phát hiện sớm sự cố cho đội ƯCSCATTTM.

- Huấn luyện, diễn tập các phương án đối phó, ứng cứu sự cố; Huấn luyện, diễn tập nâng cao kỹ năng, nghiệp vụ phối hợp, ứng cứu, chống tấn công, xử lý

mã độc, khắc phục sự cố.

- Tham mưu xây dựng, áp dụng quy trình, phương án ứng cứu sự cố của của trường, các quy định, tiêu chuẩn ATTT theo quy định.

- Phối hợp với Cục công nghệ thông tin Bộ Tư pháp tuyên truyền nâng cao nhận thức về nguy cơ, sự cố, tấn công mạng.

Điều 13. Đội trưởng Đội ứng cứu sự cố an toàn thông tin mạng

1. Chủ trì các cuộc họp, điều phối tổ chức ứng cứu; triệu tập các thành viên thường kỳ hoặc đột xuất để ngăn chặn, xử lý và khắc phục sự cố máy tính, mạng Internet.

2. Chủ trì tổ chức ứng cứu sự cố tại Trường Đại học Luật Hà Nội, điều phối, phân công các thành viên trong đội tham gia ứng cứu khi có sự cố xảy ra. Chịu trách nhiệm đầu mối liên hệ, phối hợp với Ban chỉ đạo quốc gia về ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng và các đơn vị liên quan.

3. Quyết định hình thức điều phối các hoạt động ứng cứu sự cố và chịu trách nhiệm về các yêu cầu điều phối.

Điều 14. Đội phó Đội ứng cứu sự cố an toàn thông tin mạng

1. Giúp Đội trưởng điều hành các hoạt động của Đội ƯCSCATTTM, chịu trách nhiệm trước Đội trưởng về nhiệm vụ được giao; đề xuất kế hoạch, biện pháp kỹ thuật để đảm bảo vấn đề an toàn thông tin được hiệu quả.

2. Chỉ đạo trực tiếp thành viên trong các hoạt động phòng ngừa, ngăn chặn sự cố có nguy cơ xảy ra và tích cực khắc phục khi có sự cố; thay mặt Đội trưởng điều hành các hoạt động của Đội ƯCSCATTTM khi được ủy quyền.

3. Thực hiện các nhiệm vụ cụ thể do Đội trưởng phân công và tham gia góp ý, đề xuất xây dựng kế hoạch hoạt động hàng năm của Đội ƯCSCATTTM để hoạt động hiệu quả hơn.

Điều 15. Các thành viên Đội ứng cứu sự cố an toàn thông tin mạng

1. Thực hiện các nhiệm vụ do Đội trưởng hoặc Đội phó giao.

2. Tiếp nhận và xử lý các thông báo sự cố từ các đơn vị trực thuộc trường.

3. Phản hồi các thông tin hoặc những khó khăn, vướng mắc trong quá trình thực hiện nhiệm vụ cho Đội trưởng và Đội phó để kịp thời có sự chỉ đạo, xử lý.

4. Có trách nhiệm báo cáo cơ quan quản lý khi có yêu cầu đột xuất của Cục CNTT Bộ Tư pháp hoặc khi phát hiện ra các sự cố xảy ra.

5. Tham gia đầy đủ các cuộc họp định kỳ, đột xuất và hoạt động ứng cứu sự cố khi có sự điều phối của Đội trưởng. Cung cấp thông tin liên lạc: số điện thoại cơ quan, email cho thường trực để kịp thời điều phối ứng cứu khi có sự cố xảy ra.

6. Tham gia góp ý, đề xuất xây dựng kế hoạch hoạt động hằng năm của

Đội ƯCSCATTTM.

7. Được quyền chia sẻ thông tin, kinh nghiệm, tham gia các hoạt động diễn tập, các khoá đào tạo, huấn luyện, bồi dưỡng về hoạt động ƯCSCATTTM.

Điều 16. Cơ quan quản lý thành viên của Đội ứng cứu sự cố an toàn thông tin mạng

Tạo điều kiện và ưu tiên cho viên chức, người lao động của đơn vị mình là thành viên của Đội ƯCSCATTTM thực hiện các hoạt động của Đội ƯCSCATTTM khi được triệu tập, điều phối.

CHƯƠNG V
TỔ CHỨC THỰC HIỆN

Điều 17. Điều khoản thi hành

Quy chế này được áp dụng cho Đội ƯCSCATTTM mạng tại Trường Đại học Luật Hà Nội, các cá nhân, đơn vị, tổ chức có liên quan tới hoạt động điều phối, ƯCSCATTTM. Trung tâm Công nghệ thông tin chịu trách nhiệm tham mưu triển khai thực hiện Quy chế này.

Điều 18. Khen thưởng và xử lý kỷ luật

1. Hàng năm, cơ quan Thường trực dựa trên hoạt động của mỗi thành viên để xem xét khen thưởng theo quy định hiện hành

2. Đơn vị hoặc cá nhân nào vi phạm Quy chế này, thì tuỳ theo tính chất, mức độ vi phạm có thể bị xử lý hành chính, xử lý kỷ luật hoặc các hình thức xử lý khác theo quy định của pháp luật hiện hành; nếu vi phạm gây hậu quả nghiêm trọng, làm thiệt hại tài sản, thiết bị, thông tin, dữ liệu trên mạng máy tính của Trường thì phải chịu trách nhiệm bồi thường cho những thiệt hại đã gây ra theo quy định của pháp luật./.