| BỘ THÔNG TIN VÀ TRUYỀN THÔNG | CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM<br>Độc lập - Tự do - Hạnh phúc |
|---|---|
| Số: 1620 /QĐ-BTTTT | *Hà Nội, ngày 15 tháng 10 năm 2021* |

# QUYẾT ĐỊNH
## Về việc ban hành Phương án bảo đảm, ứng phó, khắc phục sự cố an toàn, an ninh mạng đối với hệ thống thông tin dùng chung của Bộ Thông tin và Truyền thông

## BỘ TRƯỞNG BỘ THÔNG TIN VÀ TRUYỀN THÔNG

*Căn cứ Luật an toàn thông tin mạng năm 2015;*

*Căn cứ Luật an ninh mạng năm 2018;*

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

*Căn cứ Nghị định số 17/2017/NĐ-CP ngày 17/02/2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;*

*Căn cứ Kế hoạch số 3092/KH-BTTTT ngày 13/8/2021 của Bộ trưởng Bộ Thông tin và Truyền thông về việc Thực hiện Kết luận thanh tra số 09/KL-BCA ngày 14/7/2021 của Bộ Công an về việc chấp hành các quy định của pháp luật về bảo vệ bí mật nhà nước và an ninh mạng tại Bộ Thông tin và Truyền thông;*

*Căn cứ theo Quyết định số 479/QĐ-BTTTT ngày 12/4/2021 của Bộ trưởng Bộ Thông tin và Truyền thông về việc Chuyển một số nhiệm vụ từ Trung tâm Thông tin sang Trung tâm Internet Việt Nam thực hiện;*

*Căn cứ Quyết định số 1512/QĐ-BTTTT ngày 5/10/2021 của Bộ trưởng Bộ Thông tin và Truyền thông về việc ban hành Quy chế bảo đảm an toàn thông tin mạng và an ninh mạng;*

*Theo đề nghị của Giám đốc Trung tâm thông tin, Giám đốc Trung tâm Internet Việt Nam.*

## QUYẾT ĐỊNH:

**Điều 1.** Ban hành kèm theo Quyết định này Phương án bảo đảm, ứng phó, khắc phục sự cố an toàn, an ninh mạng của Bộ Thông tin và Truyền thông.

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

**Điều 3.** Chánh Văn phòng, Giám đốc Trung tâm Thông tin, Cục trưởng Cục An toàn thông tin, Giám đốc Trung tâm Internet Việt Nam và các đơn vị thuộc Bộ

LuatVietnam
Tiện ích văn bản luật

Thông tin và Truyền thông chịu trách nhiệm thi hành Quyết định này./.

***Nơi nhận:***
- Như Điều 3;
- Bộ trưởng (để b/c);
- Các Thứ trưởng;
- Lưu: VT, TTTT, VNNIC.

**KT. BỘ TRƯỞNG**
**THỨ TRƯỞNG**

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

**Nguyễn Huy Dũng**

LuatVietnam
Tiện ích văn bản luật

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

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

# PHƯƠNG ÁN BẢO ĐẢM, ỨNG PHÓ, KHẮC PHỤC SỰ CỐ AN TOÀN, AN NINH MẠNG ĐỐI VỚI HỆ THỐNG THÔNG TIN DÙNG CHUNG CỦA BỘ THÔNG TIN VÀ TRUYỀN THÔNG

*(Ban hành kèm theo Quyết định số 1620/QĐ-BTTTT ngày 15 tháng 10 năm 2021 của Bộ trưởng Bộ Thông tin và Truyền thông)*

## I. Phương án bảo đảm an toàn, an ninh mạng đối với hệ thống thông tin dùng chung của Bộ Thông tin và Truyền thông

### 1. Hồ sơ, tài liệu quản lý

a) Lập hồ sơ, tài liệu hệ thống như tài liệu thiết kế, triển khai, quản trị, vận hành, bảo đảm an toàn thông tin.

b) Lưu trữ, bảo quản hồ sơ, tài liệu, xác định phạm vi phổ biến, sử dụng của tài liệu.

c) Thực hiện cập nhật tài liệu thường xuyên khi có thay đổi, xem xét định kỳ hàng năm.

### 2. Kiểm tra, đánh giá an toàn, an ninh mạng

a) Thực hiện kiểm tra, đánh giá chức năng và an toàn, an ninh mạng các hệ thống thông tin trước khi đưa vào sử dụng khi triển khai hệ thống mới hoặc nâng cấp hệ thống có thay đổi kiến trúc của hệ thống.

b) Thực hiện kiểm tra, đánh giá chức năng và an toàn, an ninh mạng trước khi đưa vào sử dụng đối với các phần mềm thuê khoán khi xây dựng phần mềm mới hoặc khi thay đổi phần mềm, thay đổi mã nguồn mà có ảnh hưởng đến kiến trúc của phần mềm.

c) Chuẩn bị hồ sơ, thực hiện các bước, quy trình kiểm tra, đánh giá an toàn, an ninh mạng theo quy định, quy trình, hướng dẫn của đơn vị chuyên trách an toàn, an ninh mạng của Bộ Thông tin và Truyền thông.

### 3. Giám sát an toàn, an ninh mạng

a) Triển khai giám sát 24/7 đối với các hệ thống thông tin.

LuatVietnam
Tiện ích văn bản luật

b) Các yêu cầu giám sát cơ bản gồm: trạng thái hoạt động up/down; lưu lượng mạng, dịch vụ. Ngoài ra, thực hiện giám sát an toàn thông tin theo hướng dẫn tại Thông tư 31/2017/TT-BTTTT. Tùy vào điều kiện, nguồn lực và mức độ quan trọng của các hệ thống thông tin, có thể triển khai thêm các phương án giám sát khác để giám sát bất thường, nguy cơ, rủi ro hoặc dấu hiệu an toàn, an ninh mạng của hệ thống thông tin.

c) Xây dựng các quy trình xử lý đối với các sự cố an toàn, an ninh mạng được phát hiện qua công tác giám sát. Đối với các sự cố chưa có trong quy trình, có khả năng ảnh hưởng nguy hiểm tới các hệ thống thông tin quan trọng thì thực hiện cung cấp thông tin kịp thời cho đơn vị chuyên trách an toàn, an ninh mạng của Bộ Thông tin và Truyền thông để phối hợp điều tra, phân tích và xử lý.

d) Thực hiện báo cáo định kỳ, báo cáo khi có sự cố xảy ra hoặc báo cáo đột xuất theo yêu cầu của các cấp có thẩm quyền.

**4. Quản lý rủi ro**

a) Thực hiện đánh giá rủi ro đối với các hệ thống thông tin.

b) Nội dung đánh giá rủi ro tập trung xác định các điểm yếu, mối đe dọa đối với tài sản của các hệ thống thông tin, từ đó xác định hậu quả và mức độ ảnh hưởng. Đồng thời đưa ra biện pháp để xử lý rủi ro bảo đảm cân đối giữa nguồn lực và giá trị mang lại.

**5. Kết thúc vận hành, khai thác, sửa chữa, thanh lý, hủy bỏ**

a) Thực hiện hủy bỏ toàn bộ thông tin, dữ liệu trên hệ thống với sự xác nhận của đơn vị chủ quản hệ thống thông tin khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin. Trong trường hợp thông tin, dữ liệu của hệ thống thông tin lưu trữ trên tài sản vật lý, đơn vị chủ quản hệ thống thông tin thực hiện các biện pháp tiêu hủy hoặc xóa thông tin bảo đảm không có khả năng phục hồi. Với trường hợp đặc biệt không thể tiêu hủy được thông tin, dữ liệu thì sử dụng biện pháp tiêu hủy cấu trúc phần lưu trữ dữ liệu trên tài sản đó.

b) Đối với các hệ thống thông tin có dữ liệu được lưu trữ trên tài sản vật lý cần phải mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài thì phải được sự phê duyệt của cấp có thẩm quyền và thực hiện các biện pháp bảo vệ dữ liệu; Có cam

LuatVietnam
Tiện ích văn bản luật

kết bảo mật thông tin giữa bên có dữ liệu và bên cung cấp dịch vụ dịch vụ sửa chữa thiết bị lưu trữ dữ liệu.

**II. Phương án ứng phó, khắc phục sự cố an toàn, an ninh mạng đối với hệ thống thông tin dùng chung của Bộ Thông tin và Truyền thông**

**1. Nguyên tắc thực hiện**

Phương án ứng phó, khắc phục sự cố an toàn, an ninh mạng được thực hiện theo nguyên tắc: Phát hiện hoặc tiếp nhận sự cố; Xác minh, phân tích, đánh giá và phân loại sự cố; Quyết định lựa chọn phương án và phối hợp các đơn vị liên quan; Ứng cứu sự cố, khôi phục hệ thống; Điều phối, ứng cứu sự cố; Kết thúc sự cố; Khắc phục, phòng ngừa sự cố tái diễn; Hỗ trợ sau sự cố.

**2. Đánh giá các nguy cơ, sự cố an toàn, an ninh mạng**

a) Thực hiện đánh giá, xác định nguy cơ, sự cố an toàn, an ninh mạng trong hoạt động quản trị, vận hành các hệ thống thông tin.

b) Xác định phạm vi sự cố: (1) Sự cố do lỗi phần cứng, phần mềm hoặc do công tác quản trị, vận hành làm gián đoạn hệ thống thông tin. (2) Sự cố do bị tấn công mạng: tấn công từ chối dịch vụ; tấn công giả mạo; tấn công sử dụng mã độc; truy cập trái phép, chiếm quyền điều khiển; tấn công thay đổi giao diện; tấn công mã hóa phần mềm, dữ liệu, thiết bị; phá hoại thông tin, dữ liệu, phần mềm; nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu; các hình thức tấn công mạng khác.

**3. Phương án ứng phó, khắc phục đối với một số tình huống cụ thể**

a) Đối với các tình huống gây gián đoạn, ngừng dịch vụ: Trong thiết kế kỹ thuật của từng hệ thống thông tin, tùy vào mức độ quan trọng của hệ thống, có thể có các phương án triển khai chia tải (HA - High Available), dự phòng khôi phục thảm hỏa (DR). Triển khai các giải pháp, công cụ giám sát thiết bị, máy chủ, ứng dụng. Đối với hệ thống thông tin quan trọng triển khai kế hoạch sao lưu, khôi phục dữ liệu để ứng phó, khắc phục đối với tình huống bị mất/hỏng dữ liệu. Xây dựng, ban hành hồ sơ, tài liệu để chuẩn hóa hoạt động quản trị, vận hành. Kiểm soát quá trình thực hiện nâng cấp, thay đổi phần cứng, phần mềm trên hệ thống.

b) Đối với các tình huống lộ lọt thông tin hệ thống, người dùng: Thực hiện đánh giá, kiểm thử hệ thống thông tin trước khi đưa vào sử dụng, triển khai các

LuatVietnam
Tiện ích văn bản luật

biện pháp quản lý mã nguồn của phần mềm, tăng cường đào tạo nhận thức cho cán bộ, áp dụng cam kết an toàn bảo mật trong triển khai, quản trị, vận hành các hệ thống. Tùy điều kiện, nguồn lực để tiến hành triển khai các giải pháp giám sát thay đổi, bảo vệ chống tấn công như IDPS, APT, DLP, Data Encrypt, … để tăng cường phát hiện và bảo vệ.

c) Khi xảy ra các tình huống gây gián đoạn, ngừng dịch vụ hoặc lộ lọt thông tin hệ thống, người dùng, tiến hành theo dõi, phân tích thông tin, sự kiện, lưu lượng để phát hiện và thực hiện chặn lọc trên các thiết bị lớp biên mạng (gateway), liên hệ phối hợp với đơn vị cung cấp dịch vụ Internet để ngăn chặn, đơn vị cung cấp dịch vụ giám sát, đảm bảo an toàn thông tin, lực lượng chuyên trách an toàn, an ninh mạng của Bộ Thông tin và Truyền thông để phối hợp xử lý.

**4. Huấn luyện, diễn tập, phòng ngừa sự cố, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, khắc phục sự cố**

a) Tham gia các hoạt động đào tạo, huấn luyện, diễn tập theo chương trình kế hoạch của đơn vị chuyên trách/phụ trách về an toàn, an ninh mạng hoặc cơ quan, đơn vị có chuyên môn tổ chức. Tổ chức triển khai huấn luyện, diễn tập các phương án ứng phó, khắc phục sự cố với các kịch bản, tình huống sự cố cụ thể như trong mục II.3. Huấn luyện, diễn tập nâng cao kỹ năng, nghiệp vụ và hoạt động phối hợp tùy vào điều kiện nguồn lực cụ thể.

b) Triển khai nhiệm vụ nhằm phòng ngừa, giám sát phát hiện sự cố: Thực hiện nghiêm túc các biện pháp giám sát an toàn thông tin mạng; tổ chức tiếp nhận thông tin cảnh báo, nguy cơ, sự cố về an toàn, an ninh mạng; Kiểm tra, đánh giá và rà quét, bóc gỡ, phân tích, xử lý mã độc theo kế hoạch; Phòng ngừa sự cố, quản lý rủi ro; Nghiên cứu, phân tích, xác minh, cảnh báo sự cố, rủi ro, phần mềm độc hại; Xây dựng, áp dụng quy trình, quy định quản trị, vận hành; Phổ biến, nâng cao nhận thức về nguy cơ, sự cố, tấn công mạng.

c) Tùy điều kiện, nguồn lực chuẩn bị tối đa các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố: 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, tài chính để sẵn sàng đối phó, ứng

LuatVietnam
Tiện ích văn bản luật

cứu, khắc phục khi sự cố xảy ra. Tổ chức hoạt động của đội ứng cứu sự cố, bộ phận ứng cứu sự cố; thuê dịch vụ kỹ thuật và tổ chức, duy trì đội chuyên gia ứng cứu sự cố. Tham gia các hoạt động của mạng lưới ứng cứu sự cố.

**III. Vai trò, trách nhiệm**

Việc xây dựng, tổ chức và triển khai phương án bảo đảm, ứng phó, khắc phục sự cố an toàn, an ninh mạng đối với hệ thống thông tin dùng chung của Bộ Thông tin và Truyền thông do các đơn vị chủ quản hệ thống thông tin, chuyên trách an toàn thông tin và quản trị vận hành hệ thống thông tin dùng chung của Bộ Thông tin và Truyền thông thực hiện. Trách nhiệm của các đơn vị được quy định tại các Điều 20, 21, 22 của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016. Trong đó:

a) Trung tâm thông tin: là đơn vị chủ quản hệ thống thông tin dùng chung của Bộ.

b) Cục An toàn thông tin: là đơn vị chuyên trách an toàn, an ninh thông tin của Bộ.

c) Trung tâm Internet Việt Nam: là đơn vị thực hiện nhiệm vụ vận hành các hệ thống thông tin dùng chung của Bộ cho Trung tâm Thông tin.

LuatVietnam
Tiện ích văn bản luật