THÔNG TẤN XÃ VIỆT NAM
TRUNG TÂM KỸ THUẬT THÔNG TẤN

Số: 249 QĐ-TTKT

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

Hà Nội, ngày 20 tháng 9 năm 2016

QUYẾT ĐỊNH
Ban hành Quy định vận hành an toàn trung tâm dữ liệu TTXVN

GIÁM ĐỐC TRUNG TÂM KỸ THUẬT THÔNG TẤN

Căn cứ Quyết định số 74 ngày 18/02/2016 của Tổng giám đốc TTXVN về việc ban hành Quy chế công tác của Trung tâm Kỹ thuật thông tấn;

Căn cứ Quyết định số 13/QĐ-TTX của Tổng giám đốc TTXVN ngày 20/8/2009 ban hành Quy chế bảo mật hệ thống thông tin;

Theo đề nghị của các Trưởng phòng: Quản lý an toàn mạng thông tin, Quản trị hệ thống và Nghiên cứu ứng dụng.

QUYẾT ĐỊNH:

Điều 1: Ban hành kèm theo Quyết định này Quy định về vận hành an toàn trung tâm dữ liệu TTXVN

Điều 2.Các ông bà Trưởng phòng Quản lý An toàn mạng thông tin, Trưởng phòng Quản trị hệ thống và Phó trưởng phòng phụ trách Phòng Nghiên cứu ứng dụng chịu trách nhiệm thi hành Quyết định này.

Điều 3. Quyết định có hiệu lực kể từ ngày 01/10/2016/.

Nơi nhận:
- Như Điều 2;
- Lưu P Tổng hợp

GIÁM ĐỐC

TRUNG TÂM KỸ THUẬT THÔNG TẤN

Nguyễn Tuấn Hùng

THÔNG TẤN XÃ VIỆT NAM
TRUNG TÂM KỸ THUẬT
THÔNG TẤN

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

QUY ĐỊNH

Vận hành an toàn Trung tâm dữ liệu TTXVN

(Ban hành kèm theo Quyết định số 349 /QĐ-TTKT ngày 20 tháng 9 năm 2016 của Giám đốc Trung tâm Kỹ thuật thông tấn)

Điều 1: Đối tượng áp dụng.

Cán bộ, nhân viên, người thao tác kỹ thuật thuộc:

- Phòng Quản trị hệ thống.
- Phòng Nghiên cứu ứng dụng.
- Phòng Quản lý an toàn mạng thông tin.
- Các đối tác tham gia xây dựng, vận hành hệ thống kỹ thuật do Trung tâm Kỹ thuật thông tấn quản lý.

Điều 2: Phạm vi điều chỉnh

Văn bản này đưa ra những quy định, hướng dẫn chung về việc vận hành, thao tác an toàn đối với các máy chủ và thiết bị tại Trung tâm dữ liệu TTXVN ở số 5 Lý Thường Kiệt và các điểm hosting.

Mục đích của quy định này nhằm tăng khả năng đảm bảo an toàn thông tin cho hệ thống các máy chủ và thiết bị của TTXVN.

Điều 3: Giải thích từ ngữ

- Thiết bị an toàn thông tin mạng: Là phần cứng, phần mềm được thiết lập phục vụ mục đích đảm bảo an toàn, an ninh trên mạng. Bao gồm: thiết bị tường lửa, hệ thống phát hiện chống tấn công, và các thiết bị chuyên dụng cho an toàn thông tin.
- Máy chủ vận hành: Là máy chủ đang hoạt động phục vụ tác nghiệp
- Máy chủ phát triển: Là máy chủ phục vụ riêng cho công tác nghiên cứu và phát triển.
- Máy tính quản trị đặc quyền: Là máy tính dùng riêng cho công tác quản trị hệ thống.
- Máy tính kiểm thử an toàn thông tin: Là máy tính dùng riêng cho công tác kiểm thử an toàn thông tin.

Điều 4. Đối với các tác vụ quản trị hệ thống

- Người trực tiếp thao tác đối với máy chủ, các thiết bị an toàn thông tin phải thực hiện đúng quy định, quy trình và chịu trách nhiệm về vấn đề đảm bảo an toàn thông tin trong khi thao tác.
- Mỗi quản trị viên phải được cấp và sử dụng một tài khoản đăng nhập duy nhất, không dùng chung tài khoản. Tài khoản phải có mật khẩu đảm bảo an toàn theo quy định, định kỳ phải tiến hành thay đổi mật khẩu.
- Chỉ được thực hiện remote access thông qua các máy tính quản trị đặc quyền.
- Chỉ được thực hiện các tác vụ có thay đổi hệ thống trực tiếp trên máy chủ, thiết bị hoặc thông qua máy tính quản trị đặc quyền.
- Chỉ sử dụng ổ cứng di động, ổ USB đã được cấp khi thao tác; Không được sử dụng các thiết bị này cho các thao tác không liên quan tới máy chủ; Bảo quản thiết bị đúng nơi quy định.
- Việc cài đặt phần mềm lên máy chủ vận hành phải được sự đồng ý của Trưởng phòng Quản trị hệ thống.

Điều 5: Đối với thiết bị an toàn thông tin mạng.

- Phải thiết lập theo các policy base khi triển khai theo các mẫu được quy định.
- Thay đổi các tài khoản, mật khẩu mặc định của thiết bị.
- Không cho phép mở các cổng quản trị (http, https, telnet, ssh,...) thông qua môi trường Internet công cộng.
- Cập nhật đầy đủ các bản vá, nâng cấp hệ điều hành khi đủ điều kiện.
- Có phương án đảm bảo an toàn thông tin đối với các thiết bị bắt buộc phải quản trị trên môi Internet.

Điều 6: Đối với các tác vụ phát triển, chỉnh sửa phần mềm trên các hệ thống có kết nối trực tiếp Internet.

- Thiết lập trước trên máy chủ phát triển (nếu có).
- Trước khi triển khai, phải kiểm thử an toàn thông tin trên máy kiểm thử, gửi kết quả đến Phòng Quản lý an toàn mạng thông tin.
- Phòng Quản lý an toàn mạng thông tin có trách nhiệm phản hồi trong vòng 24 giờ.

Điều 7: Đối với đối tác khi thực hiện các tác vụ liên quan đến máy chủ, các thiết bị an toàn thông tin

Nếu thực hiện từ xa:

- Thực hiện đúng Quy trình Quản lý truy cập VPN.
- Chỉ được kết nối VPN tới các máy tính quản trị đặc quyền để thực hiện.

- Cán bộ trực hệ thống có nhiệm vụ ghi vào sổ trực và chạy phần mềm ghi tác vụ màn hình.

Nếu thực hiện trực tiếp:

- Thực hiện đúng Nội quy ra, vào phòng máy chủ.
- Phải được sự đồng ý của quản lý phòng chức năng. Các ông (bà) quản lý phòng chức năng liên quan có trách nhiệm cử người giám sát và chịu trách nhiệm.
- Thực hiện như điều 4.

Điều 8: Đối với các máy tính quản trị đặc quyền

- Các máy tính quản trị đặc quyền chỉ được đặt tại Phòng trực điều độ.
- Việc cài đặt thêm các phần mềm trên máy tính quản trị phải được sự đồng ý của Trưởng phòng Quản trị hệ thống.

Điều 9: Đối với máy tính kiểm thử

Phòng Quản lý an toàn mạng thông tin chịu trách nhiệm về việc đưa ra các tiêu chuẩn, quy trình và phần mềm kiểm thử trên máy tính kiểm thử.

Điều 10: Trường hợp đặc biệt

Trong các trường hợp khẩn cấp hoặc đặc biệt, không thể áp dụng các quy định trên thì phải được sự đồng ý, phê duyệt của Ban giám đốc.

GIÁM ĐỐC

TRUNG TÂM KỸ THUẬT THÔNG TẤN

Nguyễn Tuấn Hùng