Mẫu số 03
Ban hành kèm theo Thông tư số 20/2017/TT-BTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông

BÁO CÁO BAN ĐẦU SỰ CỐ MẠNG

THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO SỰ CỐ

▪ Tên tổ chức/cá nhân báo cáo sự cố (*)

▪ Địa chỉ: (*)

▪ Điện thoại (*) …….Email (*)

NGƯỜI LIÊN HỆ

▪ Họ và tên (*) …… Chức vụ:

▪ Điện thoại (*) …… Email (*)

THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ

Tên đơn vị vận hành hệ thống thông tin (*):	*Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin*				
Cơ quan chủ quản:	*Điền tên cơ quan chủ quản*				
Tên hệ thống bị sự cố	*Điền tên hệ thống bị sự cố và tên miền, địa chỉ ip liên quan*				
Phân loại cấp độ của hệ thống thông tin (nếu có)	□ Cấp độ 1	□ Cấp độ 2	□ Cấp độ 3	□ Cấp độ 4	□ Cấp độ 5
Tổ chức cung cấp dịch vụ an toàn thông tin (nếu có):	*Điền tên nhà cung cấp ở đây*				
Tên nhà cung cấp dịch vụ kết nối bên ngoài (nếu có)	*Điền tên nhà cung cấp ở đây*				
Điền tên nhà cung cấp ở đây	*Điền thông tin ở đây*				

Mô tả sơ bộ về sự cố (*)
Đề nghị cung cấp một bản tóm tắt ngắn gọn về sự cố, bao gồm đánh giá sơ bộ cuộc tấn công đã xảy ra chưa và bất kỳ các nguy cơ dẫn đến khả năng phá hoại hoặc gián đoạn dịch vụ. Cũng vui lòng xác định mức độ nhạy cảm của thông tin liên quan hoặc những đối tượng bị ảnh hưởng bởi sự cố:

Ngày phát hiện sự cố (*) (dd/mm/yy) / /	Thời gian phát hiện (*):	…… giờ.... phút

HIỆN TRẠNG SỰ CỐ (*)

□ Đã được xử lý □ Chưa được xử lý

CÁCH THỨC PHÁT HIỆN * *(Đánh dấu những cách thức được sử dụng để phát hiện sự cố)*

□ Qua hệ thống phát hiện xâm nhập □ Kiểm tra dữ liệu lưu lại (Log File)

□ Nhận được thông báo từ:

□ Khác, đó là

ĐÃ GỬI THÔNG BÁO SỰ CỐ CHO *

□ Thành viên mạng lưới chịu trách nhiệm ứng cứu sự cố cho tổ chức, cá nhân

□ ISP đang trực tiếp cung cấp dịch vụ

□ Cơ quan điều phối

THÔNG TIN BỔ SUNG VỀ HỆ THỐNG XẢY RA SỰ CỐ

▪ Hệ điều hành ……Version

▪ Các dịch vụ có trên hệ thống *(Đánh dấu những dịch vụ được sử dụng trên hệ thống)*

□ Web server □ Mail server □ Database server

□ Dịch vụ khác, đó là

▪ Các biện pháp an toàn thông tin đã triển khai *(Đánh dấu những biện pháp đã triển khai)*

□ Antivirus □ Firewall □ Hệ thống phát hiện xâm nhập

□ Khác:

▪ Các địa chỉ IP của hệ thống *(Liệt kê địa chỉ IP sử dụng trên Internet, không liệt kê địa chỉ IP nội bộ)*

▪ Các tên miền của hệ thống

▪ Mục đích chính sử dụng hệ thống

▪ Thông tin gửi kèm

□ Nhật ký hệ thống □ Mẫu virus / mã độc □ Khác:
……..

▪ Các thông tin cung cấp trong thông báo sự cố này đều phải được giữ bí mật: □ Có □ Không

KIẾN NGHỊ, ĐỀ XUẤT HỖ TRỢ

Mô tả về đề xuất, kiến nghị
Đề nghị cung cấp tóm lược về các kiến nghị và đề xuất hỗ trợ ứng cứu (nếu có)

THỜI GIAN THỰC HIỆN BÁO CÁO SỰ CỐ *: …/…/…../…(ngày/tháng/năm/giờ/phút)

CÁ NHÂN/NGƯỜI ĐẠI DIỆN THEO PHÁP LUẬT
(Ký tên, đóng dấu)

Chú thích: 1. Phần (*) là những thông tin bắt buộc. Các phần còn lại có thể loại bỏ nếu không có thông tin.

2. Sử dụng tiêu đề (subject) bắt đầu bằng "[TBSC]" khi gửi thông báo qua email

3. Tham khảo thêm tại website của VNCERT (www.vncert.gov vn)