SỞ GD&ĐT NINH THUẬN
TRƯỜNG THPT CHUYÊN LÊ QUÝ ĐÔN

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

Số: 213/QĐ-THPTLQĐ

Phan Rang – Tháp Chàm, ngày 31 tháng 10 năm 2024

QUYẾT ĐỊNH

Ban hành Quy chế về bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Trường THPT chuyên Lê Quý Đôn

HIỆU TRƯỞNG TRƯỜNG THPT CHUYÊN LÊ QUÝ ĐÔN

Căn cứ nhiệm vụ và quyền hạn của Hiệu trưởng trường THPT được quy tại Điều lệ Trường THPT ban hành kèm theo Thông tư số 32/2020/TT-BGDĐT ngày 15/9/2020 của Bộ Giáo dục và Đào tạo;

Căn cứ Thông tư 05/2023/TT-BGDĐT ngày 28/02/2023 của Bộ trưởng Bộ Giáo dục và Đào tạo về việc Ban hành Quy chế tổ chức và hoạt động của trường THPT chuyên;

Căn cứ công văn số 4567 /BGDĐT-CNTT ngày 22 tháng 8 năm 2024 của Bộ Giáo dục và Đào tạo V/v tăng cường công tác bảo vệ dữ liệu cá nhân và an toàn thông tin mạng;

Căn cứ Quyết định số 76/2024/QĐ-UBND ngày 24 tháng 9 năm 2024 Ban hành Quy chế về bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan Nhà nước trên địa bàn tỉnh Ninh Thuận;

Căn cứ Văn bản số 2628/SGDĐT-BCĐCĐS ngày 08 tháng 10 năm 2024 về việc triển khai Quyết định số 76/2024/QĐ-UBND ngày 24/9/2024 của UBND tỉnh.

Thực hiện theo công văn số 2498/SGDĐT- BCĐCĐS V/v tăng cường công tác bảo vệ dữ liệu cá nhân và an toàn thông tin mạng ngày 26 tháng 9 năm 2024 của Sở GD-ĐT Ninh Thuận;

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế về bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Trường THPT chuyên Lê Quý Đôn kể từ năm học 2024 - 2025.

Điều 2. Quyết định này có hiệu lực thi hành từ ngày 01/11/2024. Toàn thể cán bộ, viên chức, nhân viên, người lao động và học sinh nhà trường chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Trường THPT chuyên Lê Quý Đôn;
- Lưu VT

HIỆU TRƯỞNG

SỞ GIÁO DỤC VÀ ĐÀO TẠO TỈNH NINH THUẬN
TRƯỜNG TRUNG HỌC PHỔ THÔNG CHUYÊN LÊ QUÝ ĐÔN

Trần Văn Trung

QUY CHẾ

Quy chế về bảo đảm an toàn thông tin mạng và bảo vệ dữ liệu cá nhân trong hoạt động ứng dụng công nghệ thông tin của Trường THPT chuyên Lê Quý Đôn

(Ban hành Kèm theo Quyết định số 213/QĐ-THPT ngày 31 tháng 10 năm 2024 của Hiệu trưởng Trường THPT chuyên Lê Quý Đôn)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh: Quy chế này quy định về bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Trường THPT chuyên Lê Quý Đôn.

2. Đối tượng áp dụng: Tất cả cán bộ, giáo viên, nhân viên, người lao động, học sinh tham gia vận hành, khai thác các hệ thống thông tin của trường THPT chuyên Lê Quý Đôn.

Điều 2. Nguyên tắc bảo đảm an toàn thông tin

1. Các cá nhân quy định tại điều 1 của Quyết định có trách nhiệm bảo đảm an toàn thông tin là yêu cầu bắt buộc, thường xuyên, liên tục, có tính xuyên suốt quá trình liên quan đến thông tin và thiết kế, xây dựng, vận hành, nâng cấp, hủy bỏ hệ thống thông tin. Bảo đảm an toàn thông tin tuân thủ các nguyên tắc chung theo quy định.

2. Viên chức, nhân viên trong các cơ quan, đơn vị trực có trách nhiệm bảo đảm an toàn thông tin trong phạm vi xử lý công việc của mình theo quy định của Nhà nước và của Ủy ban nhân dân tỉnh với các nội dung tương ứng trong Quy chế này.

3. Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức.

Điều 3. Các hành vi nghiêm cấm

1. Các hành vi nghiêm cấm quy định tại Điều 7 Luật An toàn thông tin mạng, Điều 8 Luật An ninh mạng, Điều 5 Luật Bảo vệ bí mật nhà nước.

2. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập mạng không dây của cá nhân vào mạng nội bộ; trên cùng một thiết bị thực hiện đồng thời truy cập vào mạng nội bộ và truy cập Internet bằng thiết bị kết nối Internet của cá nhân (3G/4G, điện thoại di động, máy tính bảng, máy tính xách tay) khi cơ quan, đơn vị chủ quản hệ thống thông tin chưa cho phép.

3. Tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên thiết bị công nghệ thông tin phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc khi cơ quan, đơn vị chủ quản hệ thống thông tin chưa cho phép.

4. Tạo ra, cài đặt, phát tán phần mềm độc hại.

5. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, cá nhân khác trên môi trường mạng.

6. Các hành vi khác có tính chất cố tình làm mất an toàn, bí mật thông tin của cơ quan, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Chương II
NỘI DUNG BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 4. Các biện pháp quản lý kỹ thuật cơ bản trong công tác bảo đảm an toàn thông tin

1. Tổ chức mô hình mạng: Cài đặt, cấu hình, tổ chức hệ thống mạng theo mô hình Máy khách/Máy chủ (Client/Server), hạn chế sử dụng mô hình mạng ngang hàng. Khi thiết lập các

dịch vụ trên môi trường mạng Internet, chỉ cung cấp những chức năng thiết yếu nhất bảo đảm duy trì hoạt động của hệ thống thông tin; hạn chế sử dụng chức năng, cổng giao tiếp mạng, giao thức và các dịch vụ không cần thiết.

2. Quản lý hệ thống mạng không dây (Wireless LAN): Khi thiết lập mạng không dây, cần thiết lập các thông số an toàn và định kỳ ít nhất 3 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật.

3. Tổ chức quản lý tài khoản: Tiến hành rà soát ít nhất 6 tháng một lần các tài khoản và định danh người dùng trong hệ thống thông tin. Hủy tài khoản, quyền truy nhập hệ thống thông tin, thu hồi lại tất cả các tài sản liên quan tới hệ thống thông tin (khóa, thẻ nhận dạng, thư mục lưu trữ,...) đối với người sử dụng không còn công tác hoặc không còn sử dụng do được cấp tài khoản mới.

4. Quản lý đăng nhập hệ thống: Các hệ thống thông tin cần giới hạn số lần đăng nhập vào hệ thống, tự động khóa tài khoản khi liên tục đăng nhập sai vượt quá số lần quy định. Tổ chức theo dõi, giám sát tất cả các phương pháp đăng nhập từ xa, nhất là các trường hợp đăng nhập vào hệ thống với mục đích quản trị; yêu cầu người sử dụng đặt mật khẩu với độ an toàn cao.

5. Quản lý nhật ký sự kiện (Log File): Hệ thống thông tin cần ghi nhận các sự kiện: Quá trình đăng nhập hệ thống, các thao tác cấu hình hệ thống, quá trình truy xuất hệ thống ... Thường xuyên kiểm tra, sao lưu (backup) các nhật ký sự kiện theo từng tháng để theo dõi, xác định những sự kiện đã xảy ra của hệ thống và hạn chế việc tràn nhật ký sự kiện gây ảnh hưởng đến hoạt động của hệ thống.

6. Chống phần mềm độc hại: Triển khai các phần mềm chống mã độc trên các máy tính, thiết bị di động trong mạng để phát hiện, loại trừ phần mềm độc hại. Thường xuyên cập nhật các phiên bản mới, các bản vá lỗi của các phần mềm chống virus để bảo đảm chương trình quét virus của cơ quan trên các máy chủ, máy trạm luôn được cập nhật mới nhất; thiết lập chế độ quét thường xuyên ít nhất tuần 01 lần. Thường xuyên cập nhật bản vá các lỗ hổng bảo mật của hệ điều hành và các phần mềm ứng dụng trên máy tính để hạn chế tối đa rủi ro mất an toàn thông tin.

7. Bảo đảm an toàn cho Trang thông tin điện tử: Thực hiện theo hướng dẫn tại Công văn số 2132/BTTTT-VNCERT ngày 18/7/2011 của Bộ Thông tin và Truyền thông về việc hướng dẫn đảm bảo an toàn thông tin cho các Trang thông tin điện tử.

8. Thiết lập cơ chế sao lưu và phục hồi cho máy chủ, máy trạm: Máy chủ và máy trạm cần được thực hiện các biện pháp sao lưu dữ liệu, thông tin quan trọng nhằm phục vụ cho công tác phục hồi dữ liệu một cách nhanh nhất.

9. Xử lý khẩn cấp: Khi phát hiện hệ thống thông tin bị tấn công cần thực hiện các bước cơ bản sau:

a) Bước 1: Ngắt kết nối máy chủ ra khỏi mạng;

b) Bước 2: Sao chép nhật ký sự kiện và toàn bộ dữ liệu của hệ thống ra thiết bị lưu trữ (phục vụ cho hoạt động phân tích, điều tra);

c) Bước 3: Khôi phục hệ thống bằng cách chuyển dữ liệu sao lưu mới nhất để hệ thống hoạt động trở lại;

d) Bước 4: Chủ trì, phối hợp với các cơ quan liên quan thành lập đoàn kiểm tra an toàn thông tin định kỳ hàng năm hoặc kiểm tra đột xuất khi phát hiện có các dấu hiệu vi phạm an toàn thông tin.

Điều 5. Các biện pháp quản lý vận hành trong công tác bảo đảm an toàn thông tin

1. Đối với cán bộ chuyên trách Công nghệ thông tin (CNTT)

a) Triển khai, thực hiện các nội dung của Điều 4 Quy chế này;

b) Nắm vững và thực hiện nghiêm túc các quy định về bảo vệ bí mật Nhà nước. Thường xuyên tự cập nhật các kiến thức về an toàn thông tin, nguy cơ tiềm ẩn có thể gây mất thông tin và các biện pháp phòng tránh khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ;

c) Phối hợp chặt chẽ với cơ quan Công an trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin.

2. Đối với người sử dụng: cán bộ, viên chức, nhân viên và học sinh

a) Thường xuyên cập nhật những chính sách, quy trình, thủ tục an toàn thông tin của đơn vị cũng như thực hiện những hướng dẫn về an toàn thông tin của cán bộ chuyên trách CNTT;

b) Hạn chế việc sử dụng chức năng chia sẻ tài nguyên, khi sử dụng chức năng này cần bật thuộc tính bảo mật bằng mật khẩu và thực hiện việc thu hồi chức năng này khi đã sử dụng xong;

c) Các tài khoản đăng nhập hệ điều hành cần phải đặt mật khẩu, khi không sử dụng thì phải khóa tài khoản.

Chương III
QUY ĐỊNH BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 6. Bảo vệ bí mật nhà nước trong hoạt động ứng dụng công nghệ thông tin

1. Quy định về soạn thảo, in ấn, phát hành và sao chụp tài liệu mật

a) Không được sử dụng máy tính nối mạng internet để soạn thảo văn bản, chuyển giao, lưu trữ thông tin có nội dung thuộc bí mật nhà nước; cung cấp tin, tài liệu và đưa thông tin bí mật nhà nước trên Cổng/Trang thông tin điện tử;

b) Không được in, sao chụp tài liệu bí mật nhà nước trên các thiết bị kết nối mạng internet;

2. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các phòng, đơn vị phải báo cáo cho người có thẩm quyền. Không được cho phép các công ty tư nhân hoặc người không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố;

3. Trước khi thanh lý các máy tính trong các cơ quan nhà nước, cán bộ chuyên trách công nghệ thông tin phải dùng các biện pháp kỹ thuật xoá bỏ vĩnh viễn dữ liệu trong ổ cứng máy tính.

Điều 7. Quy định về cấp phát, thu hồi, cập nhật và quản lý các tài khoản truy cập vào hệ thống thông tin

Cán bộ quản trị mạng quản lý, cấp tài khoản cá nhân và phân quyền truy cập cho người sử dụng trên tất cả các máy trạm đặt tại các phòng, đơn vị thuộc Ban CNTT. Trong trường hợp cần thiết có thể hủy tài khoản truy cập cá nhân và ngắt kết nối đối với các hành vi cố ý tấn công hoặc gây trở ngại cho mạng máy tính; hủy quyền truy cập hệ thống thông tin đối với CB-GV-NV nghỉ chế độ, chuyển công tác và đảm bảo khả năng vẫn truy nhập được vào các hồ sơ được tạo ra bởi CB-GV-NV đó.

Hướng dẫn người sử dụng thay đổi mật khẩu ngay sau khi đăng nhập lần đầu tiên; bảo vệ thông tin của tài khoản theo quy định.

Điều 8. Cơ chế sao lưu dữ liệu

1. Cán bộ quản trị mạng phối hợp với các đơn vị có liên quan thực hiện xác định các thông tin, thực hiện quy trình sao lưu dự phòng và phục hồi cho các phần mềm, dữ liệu cần thiết theo quy định, quy trình sao lưu, lưu trữ hiện có. Các nội dung thực hiện gồm: lập danh sách các dữ liệu (thông tin cấu hình của mạng, máy chủ), phần mềm ứng dụng, cơ sở dữ liệu, tệp tin ghi nhật ký hệ được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương

pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu; thực hiện quy trình sao lưu dự phòng và phục hồi.

2. Dữ liệu sao lưu phải được lưu trữ an toàn trên Hệ thống lưu trữ dự phòng, thiết bị lưu trữ ngoài và được kiểm tra thường xuyên đảm bảo sẵn sàng cho việc sử dụng khi cần; việc kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu tối thiểu 6 tháng một lần (hoặc khi có yêu cầu đột xuất).

Điều 9. Cơ chế thông tin, báo cáo và khắc phục sự cố an toàn, an ninh thông tin

1. Đối với người sử dụng

a) Thông tin, báo cáo kịp thời cho cán bộ quản trị mạng của Ban Quản lý khi phát hiện các sự cố gây mất an toàn, an ninh thông tin mạng trong quá trình tham gia vào hệ thống thông tin;

b) Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

2. Đối với cán bộ quản trị mạng

a) Áp dụng mọi biện pháp để khắc phục và hạn chế thiệt hại do sự cố xảy ra, lập biên bản báo cáo Ban Giám hiệu Trường THPT Chuyên Lê Quý Đôn;

b) Cung cấp đầy đủ, chính xác, kịp thời những thông tin cần thiết; thực hiện theo đúng hướng dẫn và tạo điều kiện thuận lợi cho cơ quan chức năng (Công an tỉnh, Trung tâm ứng cứu sự cố mạng, máy tính Việt Nam VNCert...) tham gia khắc phục sự cố.

Chương VI

TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN VÀ CHẾ ĐỘ BÁO CÁO KIỂM TRA ĐỊNH KỲ VÀ ĐỘT XUẤT

Điều 10. Trách nhiệm của lãnh đạo nhà trường

a) Khi có sự cố hoặc nguy cơ mất an toàn thông tin, kịp thời sử dụng cán bộ chuyên trách về an toàn, an ninh thông tin của cơ quan áp dụng mọi biện pháp kỹ thuật để khắc phục, hạn chế thấp nhất mức thiệt hại có thể xảy ra;

b) Tạo điều kiện thuận lợi cho các cơ quan chức năng tham gia khắc phục sự cố và thực hiện đúng theo hướng dẫn;

c) Phân công cán bộ chuyên trách về an toàn hệ thống thông tin, đảm bảo an ninh thông tin, bảo mật trước khi tiến hành các hoạt động quản lý, vận hành hệ thống thông tin. Tạo điều kiện cho cán bộ chuyên trách được học tập, tiếp thu công nghệ và kiến thức về an toàn bảo mật thông tin.

Điều 11. Trách nhiệm của người sử dụng

1. Nghiêm chỉnh chấp hành các quy định, quy trình về an toàn, an ninh thông tin của Ban CNTT cũng như quy định khác của pháp luật, nâng cao ý thức cảnh giác và trách nhiệm bảo đảm an toàn, an ninh thông tin tại cơ quan, đơn vị.

2. Khi phát hiện sự cố phải báo ngay với lãnh đạo trường và nhân viên quản trị mạng để kịp thời ngăn chặn, xử lý.

3. Hưởng ứng, tham gia các chương trình đào tạo, hội nghị về an toàn, an ninh thông tin mạng.

4. Có trách nhiệm quản lý, bảo quản thiết bị được giao sử dụng; không tự ý thay đổi cấu hình hoặc tháo lắp các thiết bị trên máy tính khi chưa có sự đồng ý của Lãnh đạo trường.

5. Định kì, ít nhất 3 tháng phải thay đổi mật khẩu cho các tài khoản của mình. Sử dụng mật khẩu có độ an toàn tối đa theo qui định của hệ thống: Hãy tạo mật khẩu dài, bao gồm cả chữ hoa, chữ thường, số và ký tự đặc biệt. Tránh sử dụng các thông tin dễ đoán như ngày sinh hay tên.

6. Thường xuyên kiểm tra các tài khoản trực tuyến được cấp để phát hiện sớm các hoạt động đáng ngờ.

7. Cẩn thận với email và liên kết lạ: Tránh mở email từ người gửi không rõ ràng hoặc nhấp vào các liên kết không xác định.

8. Không chuyển giao tài khoản và mật khẩu của mình cho người khác để nhờ làm giùm công việc của mình.

9. Không cung cấp dữ liệu cá nhân mình cũng như của người khác (mà chưa được sự đồng ý của họ) lên môi trường mạng xã hội.

Điều 12. Trách nhiệm của nhân viên quản trị mạng

1. Nhân viên quản trị mạng do Hiệu trưởng Trường THPT chuyên Lê Quý Đôn phân công, chịu trách nhiệm quản lý, vận hành các hoạt động hệ thống mạng máy tính. Tham mưu cho Ban Giám hiệu Trường THPT chuyên Lê Quý Đôn trong việc đầu tư thiết bị phần cứng, phần mềm, công tác bảo mật thông tin trên môi trường mạng; sử dụng phần mềm có bản quyền và phần mềm mã nguồn mở cho hệ thống máy tính; cập nhật cấu hình chuẩn cho các thành phần của hệ thống khi tiến hành cài đặt và thiết lập cấu hình chặt chẽ nhất cho các sản phẩm an toàn thông tin nhưng vẫn duy trì yêu cầu hoạt động của hệ thống thông tin.

2. Sao chép, lưu trữ thông tin tại nơi an toàn; kiểm tra thông tin sao lưu để đảm bảo tính sẵn sàng và toàn vẹn của thông tin. Xử lý các sự cố về an toàn, an ninh thông tin và bảo mật hệ thống thông tin.

3. Triển khai các biện pháp chống virus, thư rác cho hệ thống máy chủ và tại các máy trạm, các thiết bị di động trong mạng của Ban Quản lý. Sử dụng biện pháp chống virus, thư rác để phát hiện và loại trừ những đoạn mã độc (virus, trojan.,.) được truyền tải bởi: thư điện tử, tập tin đính kèm từ Internet, thiết bị lưu trữ tháo lắp để khai thác lỗ hổng của hệ thống thông tin, Thường xuyên cập nhật các phần mềm chống virus, thư rác, bản vá lỗi hệ thống và hướng dẫn người dùng (user) sử dụng chương trình để bảo vệ an toàn dữ liệu.

4. Theo dõi và quản lý hoạt động hệ thống mạng, đề xuất lựa chọn công nghệ và triển khai các giải pháp nhằm đảm bảo cho hệ thống mạng cục bộ (LAN) hoạt động thông suốt, đảm bảo an toàn và bảo mật các thông tin truyền dẫn cho hệ thống mạng máy tính và đảm bảo hệ thống mạng LAN luôn được kết nối, hoạt động thông suốt.

5. Trực tiếp cài đặt, quản lý các phần mềm hệ thống và phần mềm ứng dụng trong hệ thống mạng máy tính; nghiên cứu, đề xuất, nâng cấp công nghệ phần mềm theo định hướng quản lý Nhà nước của ngành và tuân theo quy định của Chính phủ. Lắp đặt, hướng dẫn sử dụng, nâng cấp, cập nhật, bảo trì và quản trị mạng máy tính đảm bảo hoạt động ổn định và an toàn cho người sử dụng. Kiểm tra và xử lý các lỗi kỹ thuật đảm bảo việc truyền, nhận thông tin thông suốt trong giáo viên. Giữ bí mật tuyệt đối các thông tin trên mạng.

6. Thực hiện việc đánh giá, báo cáo và đề xuất với Ban Giám hiệu Trường THPT chuyên Lê Quý Đôn các biện pháp phòng chống các rủi ro và mức độ nghiêm trọng của rủi ro đối với hệ thống thông tin của cơ quan (các rủi ro có thể xảy ra do sự truy cập, sử dụng thông tin trái phép; mất thông tin; thay đổi hoặc phá hủy thông tin của hệ thống).

Điều 13. Chế độ báo cáo, kiểm tra định kỳ và đột xuất

1. Ban Giám hiệu Trường THPT chuyên Lê Quý Đôn báo cáo tình hình an toàn, an ninh thông tin gửi cấp trên theo quy định.

2. Phối hợp với Sở Thông tin và Truyền thông và các đơn vị có liên quan tiến hành kiểm tra công tác đảm bảo an toàn, an ninh thông tin mạng.

3. Phối hợp với đoàn kiểm tra tiến hành kiểm tra đột xuất các cá nhân có dấu hiệu vi phạm an toàn, an ninh thông tin.

Điều 14. Khen thưởng và xử lý vi phạm

1. Cán bộ, viên chức, người lao động và học sinh thực hiện tốt Quy chế này sẽ được xem xét đánh giá khen thưởng.

2. Cán bộ, viên chức, người lao động và học sinh có hành vi vi phạm quy chế này thì tùy theo tính chất, mức độ vi phạm bị xử lý kỷ luật. Nếu gây thiệt hại có tính chất nghiêm trọng thì phải bồi thường về vật chất và bị truy cứu trách nhiệm hình sự theo quy định của Pháp luật hiện hành.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 17. Điều khoản thi hành

Trong quá trình thực hiện Quy chế này nếu phát hiện những điều không phù hợp, vướng mắc cần sửa đổi, bổ sung, các cá nhân kịp thời báo cáo về văn phòng để tổng hợp trình Ban Giám hiệu Trường THPT chuyên Lê Quý Đôn xem xét, điều chỉnh, bổ sung cho phù hợp./.

MẪU SỐ 01

SỞ GD&ĐT NINH THUẬN
TRƯỜNG THPT CHUYÊN LÊ QUÝ ĐÔN

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

Phan Rang – Tháp Chàm, ngày ... tháng ... năm ...

BÁO CÁO SỰ CỐ AN TOÀN THÔNG TIN 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 1	☐ Cấp 2	☐ Cấp 3	☐ Cấp 4	☐ Cấp 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*				
Dải địa chỉ Public IP kết nối với hệ thống bên ngoài:	*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 dân 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/yyyy) ...../...../.....	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):

NGƯỜI THỰC HIỆN

(Ký tên)

MẪU SỐ 02

SỞ GD&ĐT NINH THUẬN
TRƯỜNG THPT CHUYÊN LÊ QUÝ ĐÔN

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

Phan Rang – Tháp Chàm, ngày ... tháng ... năm ...

BÁO CÁO KẾT THÚC ỨNG PHÓ SỰ CỐ

THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO

- Tên tổ chức/cá nhân báo cáo sự cố (*) .....
- Địa chỉ: (*) .....
- Điện thoại (*) ..... Email (*) .....

KÝ HIỆU BÁO CÁO BAN ĐẦU SỰ CỐ

Số ký hiệu..... Ngày báo cáo: / / 20....

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*				
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*
Tên/Mô tả về sự cố					
Ngày phát hiện sự cố / / (dd/mm/yy)		Thời gian phát hiện (*):		.... giờ.... phút	
Kết quả xử lý sự cố					
Cung cấp, tóm tắt tổng quát về những gì đã xảy ra và cách thức giải quyết, đề xuất giải pháp ứng cứu ứng sự cố nhằm xử lý nhanh sự cố, giảm nhẹ rủi ro và thiệt hại đối với sự cố tương tự trong tương lai...					
Các tài liệu đính kèm Liệt kê các tài liệu liên quan (báo cáo diễn biến sự cố; phương án xử lý, log file….)					

NGƯỜI THỰC HIỆN
(Ký tên)