BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC NHA TRANG

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

Số: 725 / QĐ-ĐHNT

Khánh Hòa, ngày 20 tháng 5 năm 2026

QUYẾT ĐỊNH
Ban hành Quy định An ninh mạng của Trường Đại học Nha Trang

HIỆU TRƯỞNG TRƯỜNG ĐẠI HỌC NHA TRANG

Căn cứ Quyết định số 155/CP ngày 16/8/1966 của Hội đồng Chính phủ về việc thành lập và quy định nhiệm vụ, quyền hạn của Trường Thủy sản, nay là Trường Đại học Nha Trang;

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

Căn cứ Luật Bảo vệ dữ liệu cá nhân ngày 26/6/2025;

Căn cứ Luật Giáo dục đại học ngày 10/12/2025;

Căn cứ Luật An ninh mạng ngày 10/12/2025;

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 và Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP;

Căn cứ Quyết định số 3238/QĐ-BGDĐT ngày 30/10/2024 của Bộ Giáo dục và Đào tạo ban hành Quy chế quản lý và sử dụng mạng máy tính đảm bảo an ninh mạng của Bộ Giáo dục và Đào tạo;

Căn cứ Nghị quyết số 32/NQ-ĐHNT ngày 03/12/2024 của Hội đồng trường ban hành Quy chế Tổ chức và hoạt động của Trường Đại học Nha Trang; Nghị quyết số 13/NQ-ĐHNT ngày 10/7/2025 và Nghị quyết số 33/NQ-ĐHNT ngày 12/12/2025 về việc sửa đổi, bổ sung Quy chế Tổ chức và hoạt động của Trường Đại học Nha Trang;

Căn cứ Quyết định số 100/QĐ-ĐHNT ngày 22/01/2026 của Hiệu trưởng ban hành Quy định nhiệm vụ, quyền hạn của các đơn vị thuộc và trực thuộc Trường Đại học Nha Trang;

Theo đề nghị của Trưởng phòng Hạ tầng và Công nghệ Thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy định an ninh mạng của Trường Đại học Nha Trang.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày 01/7/2026.

Điều 3. Trưởng phòng Hạ tầng và Công nghệ thông tin, các Trưởng đơn vị và cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Ban Giám hiệu (để c/đ);
- Như Điều 3;
- Lưu: VT, HTCN.

HIỆU TRƯỞNG

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC NHA TRANG

Quách Hoài Nam

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC NHA TRANG

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

QUY ĐỊNH
An ninh mạng của Trường Đại học Nha Trang

(*Kèm theo Quyết định số 725 /QĐ-ĐHNT ngày 20 tháng 5 năm 2026 của Hiệu trưởng Trường Đại học Nha Trang*)

Chương I
QUY ĐỊNH CHUNG

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

1. Quy định này quy định về an ninh mạng, bảo vệ dữ liệu cá nhân và an toàn thông tin của hệ thống công nghệ thông tin (CNTT) và chuyển đổi số của Trường Đại học Nha Trang (sau đây gọi tắt là Trường hoặc Nhà trường).

2. Quy định này áp dụng đối với các đơn vị thuộc và trực thuộc Trường; viên chức, người lao động (VC, NLĐ), sinh viên, học viên, nghiên cứu sinh (gọi chung là người học) của Nhà trường và các tổ chức, cá nhân có liên quan đến công tác an ninh mạng, an toàn thông tin của Trường.

Điều 2. Mục đích của Quy định

1. Đảm bảo các hoạt động trên không gian mạng của Nhà trường tuân thủ đúng theo quy định pháp luật hiện hành của cấp có thẩm quyền.

2. Quy định bảo mật dữ liệu cá nhân của VC, NLĐ và người học, bảo mật dữ liệu Nhà trường.

3. Nhận diện các rủi ro ảnh hưởng đến an toàn hệ thống CNTT Nhà trường.

4. Quy định các điều kiện cho các yếu tố về quy trình, nhân lực, kỹ thuật để đảm bảo hệ thống mạng và hệ thống thông tin Nhà trường vận hành ổn định, an toàn trong các sự cố tấn công mạng hay sự cố hư hỏng thiết bị.

5. Các vấn đề liên quan đến phân quyền và quản lý sử dụng cho từng phần mềm cụ thể được quy định trong Quy định về quản lý, khai thác, vận hành và phân quyền sử dụng các phần mềm quản lý của Trường.

Điều 3. Giải thích từ ngữ

1. *An ninh mạng*: đảm bảo các hoạt động trên không gian mạng tuân thủ đúng theo pháp luật Nhà nước.

2. *An toàn thông tin*: đảm bảo hạ tầng CNTT và hệ thống thông tin Nhà trường vận hành ổn định, ngăn ngừa và xử lý các tình huống tấn công mạng, các rủi ro dẫn đến hư hỏng và mất mát thông tin dữ liệu Nhà trường.

3. *Bảo mật thông tin dữ liệu*: là việc áp dụng phân quyền, các quy trình nghiệp vụ và các biện pháp kỹ thuật như mã hóa dữ liệu nhằm đảm bảo các thông tin dữ liệu Nhà trường, thông tin cá nhân của VC, NLĐ và người học được bảo mật, không bị tiết lộ ra bên ngoài.

4. *Hạ tầng công nghệ thông tin*: là các thiết bị phần cứng và phần mềm nền tảng giúp triển khai các phần mềm ứng dụng và chuyển đổi số.

5. *Hệ thống thông tin*: bao gồm tất cả các phần mềm và thông tin dữ liệu của các phần mềm ứng dụng trong công tác đào tạo và quản trị Nhà trường. Các phần mềm này được triển khai tại Phòng máy chủ Nhà trường hoặc dịch vụ thuê ngoài.

6. *Phần mềm mã độc*: là các phần mềm thuộc dạng virus máy tính, được tạo ra với mục đích lan truyền trên mạng nhằm thực hiện tấn công mạng và phá hoại dữ liệu.

7. *Thông tin, dữ liệu và tài sản số*: là các dữ liệu về các hoạt động của Nhà trường đã được số hóa và lưu trữ trên phần mềm, được xử lý bằng máy tính và có khả năng chia sẻ cho các đối tượng liên quan.

8. *Tấn công mạng: là các hành vi truy cập hệ thống thông tin Nhà trường từ bên* trong hay bên ngoài Trường, thực hiện các hành vi phá hoại như làm quá tải hệ thống, phát tán thông tin rác, lấy trộm thông tin dữ liệu, sửa đổi hoặc xóa dữ liệu, hoặc mã hóa dữ liệu đòi tiền chuộc.

Chương II
AN NINH HOẠT ĐỘNG TRÊN KHÔNG GIAN MẠNG

Điều 4. Các thành phần không gian mạng Trường Đại học Nha Trang

1. Hạ tầng CNTT bao gồm phòng máy chủ, hệ thống mạng nội bộ và các thiết bị ngoại vi, thiết bị có kết nối mạng Internet.

2. Hệ thống các phần mềm ứng dụng trong hoạt động giảng dạy, đào tạo.

3. Hệ thống các phần mềm ứng dụng trong hoạt động quản trị Nhà trường.

4. Hệ thống website Trường, bao gồm website chính ntu.edu.vn và website các đơn vị.

5. Mạng xã hội Nhà trường trên các kênh truyền thông như Facebook, Youtube, Zalo,…

Điều 5. Các hành vi không được phép thực hiện trên không gian mạng Nhà trường

1. Tuyên truyền các nội dung chống phá Nhà nước; các nội dung trái với thuần phong mỹ tục; các nội dung xấu, độc; các thông tin sai sự thật, ảnh hưởng đến uy tín và quyền lợi của các tổ chức, cá nhân khác.

2. Tuyên truyền các thông tin sai sự thật về Trường, xúc phạm uy tín VC, NLĐ và người học tại Trường.

3. Phá hoại không gian mạng Nhà trường, bao gồm các thiết bị CNTT vật lý và các hệ thống phần mềm.

4. Tấn công mạng Nhà trường, lấy trộm thông tin dữ liệu hoặc sửa đổi, phá hoại dữ liệu trong các hệ thống phần mềm.

5. Sử dụng hệ thống mạng Nhà trường cho các hành vi vi phạm pháp luật, tấn công mạng các tổ chức, cá nhân khác (phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo,…).

6. Các hành vi khác không được phép thực hiện theo quy định pháp luật hiện hành có liên quan.

Điều 6. Các hành vi khuyến khích thực hiện trên không gian mạng Nhà trường

1. Nhận diện, đánh giá đúng/sai các thông tin lan truyền trên mạng, không truyền thông các thông tin sai lệch. Cảnh giác với các hành vi bất thường tiềm ẩn các nguy cơ dẫn đến lừa đảo cá nhân hoặc lợi dụng để lừa đảo người khác.

2. Bảo mật các tài khoản cá nhân (máy tính, phần mềm, website, mạng xã hội,...) tránh bị người khác lợi dụng để thực hiện các hành vi không được phép hoặc vi phạm pháp luật.

3. Cẩn thận rà soát khi truy cập các liên kết website và quét các mã QR lạ, nhất là được gửi từ các email giả mạo, từ mạng xã hội. Không truy xuất liên kết website hoặc quét mã QR khi chưa kiểm chứng được nguồn gốc xuất xứ.

4. Phản ánh kịp thời cho các đơn vị có trách nhiệm theo quy định khi phát hiện các cá nhân có các hành vi vi phạm được nêu tại Điều 5 của Quy định này.

Điều 7. Các không gian mạng khác

VC, NLĐ và người học của Trường khi tham gia các không gian mạng thuộc các tổ chức khác cần tuân thủ theo quy định của các tổ chức đó và theo quy định của pháp luật Nhà nước.

Chương III
RỦI RO AN TOÀN THÔNG TIN

Điều 8. Rủi ro tiết lộ thông tin dữ liệu Nhà trường

1. Thông tin dữ liệu cá nhân của VC, NLĐ và người học, thông tin dữ liệu Nhà trường có thể bị tiết lộ ra bên ngoài và bị lợi dụng để thực hiện các hành vi vi phạm pháp luật gây ảnh hưởng đến cá nhân và Nhà trường.

2. Rủi ro tiết lộ thông tin dữ liệu có các nguyên nhân chính: (1) người được phân quyền quản lý dữ liệu cố ý hoặc vô ý tiết lộ thông tin, (2) hệ thống thông tin Nhà trường bị tấn công mạng để đánh cắp dữ liệu.

Điều 9. Rủi ro tấn công mạng và lây nhiễm mã độc

1. Hệ thống CNTT Nhà trường có thể bị tấn công phá hoại từ bên trong và bên ngoài, bị lây nhiễm mã độc dẫn đến các sự cố như gián đoạn, quá tải hạ tầng CNTT; thông tin bị đánh cắp; dữ liệu bị làm cho sai lệch hoặc mất mát dữ liệu.

2. Rủi ro tấn công mạng xảy ra do ba nguyên nhân chính: (1) sử dụng các thiết bị phần cứng/phần mềm có lỗi bảo mật, (2) người sử dụng không tuân thủ theo quy trình bảo mật, (3) do sơ suất trong quản lý vận hành hệ thống.

Điều 10. Rủi ro hư hỏng thiết bị

1. Các thiết bị phần cứng thuộc hạ tầng CNTT (máy tính, thiết bị mạng, thiết bị lưu trữ, …) có khả năng xảy ra hư hỏng dẫn đến gián đoạn, tạm dừng hoạt động CNTT trong khoảng thời gian ngắn hoặc dài ngày.

2. Các thiết bị lưu trữ dữ liệu bị hư hỏng có khả năng gây mất mát thông tin dữ liệu nếu không có chế độ sao lưu dữ liệu dự phòng.

3. Rủi ro trong môi trường vận hành như thiên tai, bão lụt, sét đánh, độ ẩm, nhiệt độ, cháy nổ, sự mất ổn định nguồn điện,… có thể dẫn đến hư hỏng thiết bị.

Chương IV
BẢO MẬT DỮ LIỆU CÁ NHÂN VÀ DỮ LIỆU NHÀ TRƯỜNG

Điều 11. Dữ liệu cá nhân và dữ liệu Nhà trường

1. Dữ liệu cá nhân VC, NLĐ và người học: là những thông tin dữ liệu được thu thập trong quá trình tuyển dụng, tuyển sinh phục vụ công tác quản lý của Nhà trường; các thông tin dữ liệu phát sinh trong quá trình công tác, học tập tại Trường, gồm các loại dữ liệu sau:

a) Dữ liệu liên quan quá trình công tác và quá trình học tập tại Trường, bảng lương, bảng điểm,…

b) Dữ liệu liên quan nhân thân của cá nhân như số căn cước công dân, tài khoản ngân hàng, địa chỉ, số điện thoại, mật khẩu tài khoản dưới dạng mã hóa, thông tin sức khỏe y tế, thông tin người thân,…

2. Các loại dữ liệu khác không xếp vào dữ liệu cá nhân được xác định chung là thông tin dữ liệu Nhà trường.

Điều 12. Bảo mật thông tin dữ liệu

1. Bảo mật dữ liệu cá nhân của VC, NLĐ và người học được thực hiện theo Luật Bảo vệ dữ liệu cá nhân và các quy định pháp luật hiện hành có liên quan.

2. Các loại thông tin dữ liệu không thuộc diện bảo mật thông tin dữ liệu bao gồm: thông tin thuộc phạm vi ba công khai theo quy định của Nhà nước, các thông tin tra cứu văn bằng chứng chỉ của người học, các thông tin đăng tải trên website, thông tin phục vụ quảng bá tuyển sinh và các thông tin khác có sự đồng ý của Ban Giám hiệu Nhà trường.

3. Các loại thông tin không thuộc Khoản 2 Điều này được hiểu là thuộc phạm vi bảo mật dữ liệu, chỉ đơn vị hoặc cá nhân được phân quyền mới có thể xem và xử lý dữ liệu theo Quy định về quản lý, khai thác, vận hành và phân quyền sử dụng các phần mềm quản lý của Trường.

4. Đơn vị hoặc cá nhân được phân quyền truy cập dữ liệu theo chức năng nhiệm vụ có trách nhiệm bảo mật các thông tin dữ liệu, tránh để lộ thông tin ra bên ngoài.

5. Mật khẩu người dùng và mật khẩu hệ thống phải đảm bảo độ khó để tránh bị phỏng đoán hoặc tấn công vét cạn (mật khẩu dài hơn 08 ký tự, có đủ chữ cái hoa, thường, chữ số, ký tự đặc biệt), đổi mật khẩu thường xuyên 06 tháng một lần và sử dụng các phương pháp xác thực hai lớp.

6. Khi VC, NLĐ thôi việc, nghỉ hưu, chuyển công tác, chuyển đổi vị trí việc làm trong Trường, bộ phận chuyên trách CNTT cần hủy phân quyền và khóa tài khoản các phần mềm tương ứng.

7. Các thiết bị CNTT khi hư hỏng hoặc thay thế phải bàn giao về bộ phận chuyên trách CNTT thực hiện xóa dữ liệu trước khi đưa đi sửa chữa hoặc thanh lý.

Điều 13. Bảo mật kết nối dữ liệu với các đối tác

1. Các đối tác kết nối dữ liệu với Nhà trường được hiểu là các đối tác hợp tác hai bên cùng có lợi hoặc các đối tác được Nhà trường trả phí để cung cấp dịch vụ. Ví dụ:

các ngân hàng cung cấp dịch vụ thu học phí, đơn vị cung cấp hóa đơn điện tử, chữ ký số, kết nối liên thông trục văn bản quốc gia,…

2. Kết nối dữ liệu cần đảm bảo các yêu cầu kỹ thuật sau:

a) Mã hóa dữ liệu gửi và nhận với đối tác.

b) Áp dụng chữ ký số với những dữ liệu quan trọng.

c) Khi cần chứng thực người sử dụng, việc chứng thực thực hiện tại hệ thống máy chủ Nhà trường. VC, NLĐ và người học không thực hiện chứng thực, nhập mật khẩu tài khoản trên hệ thống của đối tác.

3. Có cam kết về bảo mật dữ liệu của các bên liên quan.

4. Đối với các phần mềm theo dạng thuê dịch vụ, hệ thống thông tin được cài đặt tại máy chủ của nhà cung cấp, cần phải có cam kết các điều kiện về bảo mật dữ liệu và phòng chống tấn công mạng, điều kiện về sao lưu dữ liệu và hủy bỏ dữ liệu trên máy chủ nhà cung cấp khi kết thúc hợp đồng.

Chương V
ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 14. Vận hành theo tiêu chuẩn an toàn hệ thống thông tin cấp độ 3

1. Hệ thống thông tin Trường Đại học Nha Trang được xác định thuộc mức an toàn hệ thống thông tin cấp độ 3 (hệ thống thông tin phục vụ người dân, cung cấp dịch vụ trực tuyến khác có xử lý thông tin riêng, thông tin cá nhân của từ 10.000 người sử dụng trở lên).

2. Các bước thực hiện vận hành theo tiêu chuẩn an toàn hệ thống thông tin cấp độ 3:

a) Rà soát các quy trình vận hành hệ thống thông tin nhằm đáp ứng các yêu cầu của tiêu chuẩn.

b) Xây dựng hồ sơ đăng ký an toàn hệ thống thông tin cấp độ 3 và trình Bộ Giáo dục và Đào tạo phê duyệt.

c) Định kỳ kiểm tra đảm bảo các quy trình vận hành hệ thống thông tin tuân thủ theo các yêu cầu của hồ sơ đã được phê duyệt.

Điều 15. An toàn thông tin máy tính và thiết bị ngoại vi

1. Máy tính và thiết bị ngoại vi được hiểu là các máy tính để bàn, máy tính xách tay, máy in,… là tài sản của Nhà trường, được cấp cho VC, NLĐ sử dụng thông qua kết nối mạng cục bộ (mạng LAN).

2. Máy tính cá nhân phải sử dụng các phần mềm có bản quyền, không được cài đặt các phần mềm bẻ khóa, phần mềm không rõ nguồn gốc. Chỉ cài đặt các phần mềm phục vụ công tác. Phần mềm phòng chống virus và tường lửa máy tính luôn trong trạng thái bật. Người dùng không được tự ý thay đổi cấu hình máy tính cũng như cài đặt các phần mềm ngoài danh sách Nhà trường quy định.

3. Người dùng chỉ sử dụng máy tính cho các hoạt động công vụ, không truy cập các website có nội dung xấu, độc, tiềm ẩn nguy cơ lây nhiễm mã độc vào máy tính và hệ thống mạng Nhà trường, cẩn thận rà soát khi truy cập các liên kết website lạ, nhất là các liên kết từ các email giả mạo.

4. Thông báo ngay cho bộ phận chuyên trách CNTT khi phát hiện những vấn đề bất thường (máy chạy chậm bất thường, các cảnh báo từ các phần mềm phòng chống virus,…) để được xử lý kịp thời.

5. Định kỳ sao lưu các file dữ liệu cá nhân đề phòng hư hỏng máy tính cá nhân và có trách nhiệm bảo mật file dữ liệu đã được sao lưu.

6. Các thiết bị không phải là tài sản Nhà trường, bao gồm máy tính xách tay, điện thoại di động cá nhân, được truy cập mạng wifi Nhà trường để truy cập Internet và sử dụng các phần mềm Nhà trường theo tiêu chuẩn truy cập công cộng ở bên ngoài Trường. Hệ thống mạng Nhà trường có khả năng truy vết các truy cập wifi này để phát hiện các trường hợp sử dụng mạng Nhà trường cho các hành vi phá hoại.

7. Cá nhân không được tự ý gắn các thiết bị ngoại vi (bộ chia mạng, thiết bị phát sóng wifi,…) vào hệ thống mạng nội bộ của Trường mà không có sự đồng ý của bộ phận chuyên trách CNTT.

Điều 16. An toàn thông tin phòng máy chủ và hệ thống mạng

1. Hệ thống mạng và phòng máy chủ phải được thiết kế theo mô hình phân lớp bảo mật gồm các vùng nghiêm ngặt, vùng DMZ, vùng công cộng theo các quy tắc thiết kế hệ thống mạng. Việc nâng cấp bổ sung hệ thống mạng và phòng máy chủ phải đảm bảo yêu cầu về an toàn thông tin khi trang bị và khi đưa vào sử dụng.

2. Việc định tuyến vào/ra hệ thống mạng và các cổng dịch vụ máy chủ thực hiện theo nguyên tắc: mặc định là không cho phép, chỉ cho phép khi có nhu cầu, cho phép vừa đủ không dư thừa để không bị lợi dụng cho các hành vi phá hoại.

3. Phải lưu nhật ký khi thay đổi cấu hình kỹ thuật của các thiết bị mạng và máy chủ.

4. Phòng máy chủ phải có hệ thống giám sát vào ra và phải ghi nhật ký kiểm tra giám sát. Kiểm tra giám sát vận hành phòng máy chủ định kỳ để kịp thời phát hiện các trường hợp bất thường, các hư hỏng thiết bị.

5. Hệ thống dây mạng và thiết bị mạng tại các khu vực trong Trường phải lắp đặt trong ống, máng, có tủ che đậy kín, hạn chế khả năng tiếp cận trái phép vào dây dẫn hoặc cổng mạng.

6. Thường xuyên cập nhật các bản vá lỗi thiết bị, vá lỗi hệ điều hành nhằm ngăn chặn tấn công mạng trên lỗi thiết bị.

7. Trang bị hệ thống tường lửa nhằm phát hiện và ngăn ngừa tự động các tấn công mạng và mã độc phổ biến.

Điều 17. An toàn thông tin trang bị và vận hành phần mềm

1. Các phần mềm cài đặt trên máy chủ (hệ điều hành, phần mềm hệ thống, phần mềm ứng dụng của Trường) phải sử dụng phần mềm có bản quyền, không sử dụng phần mềm bẻ khóa và không rõ nguồn gốc.

2. Các hệ thống phần mềm trước khi đưa vào sử dụng phải thực hiện kiểm thử bảo mật nhằm hạn chế tối đa lỗi bảo mật. Cụ thể như sau:

- Dữ liệu luân chuyển trong mạng nội bộ và mạng Internet phải được mã hóa trong quá trình truyền dữ liệu.

- Có khả năng ngăn chặn các loại hình tấn công phần mềm phổ biến như SQL Injection, XSS, upload file, CSRF,…

- Có thực hiện phân quyền và ghi nhật ký các thao tác chỉnh sửa dữ liệu tối thiểu trong 03 tháng gần nhất.

3. Thường xuyên thay đổi mật khẩu hệ điều hành, mật khẩu cơ sở dữ liệu, mật khẩu quản trị hệ thống (tối thiểu phải thay đổi 06 tháng một lần).

4. Thường xuyên cập nhật các bản vá lỗi phần mềm do nhà sản xuất cung cấp.

5. Công tác xây dựng phần mềm, kiểm thử, sửa lỗi, nâng cấp phần mềm (nhà cung cấp phần mềm bên ngoài hoặc đơn vị bên trong Trường tự xây dựng) phải được tiến hành trên môi trường thử nghiệm độc lập hoàn toàn với môi trường vận hành chính thức.

Điều 18. Đảm bảo an toàn thiết bị hoạt động liên tục khi có sự cố hư hỏng

1. Thiết kế hệ thống mạng và phòng máy chủ Nhà trường phải có tính dự phòng, phải có thiết bị thay thế để tránh gây gián đoạn và tạm dừng hệ thống CNTT khi có sự cố.

2. Hệ thống thiết bị lưu trữ phải áp dụng các tiêu chuẩn dự phòng tối thiểu RAID-1, RAID-5, RAID-6 nhằm đảm bảo không gián đoạn và mất mát dữ liệu tức thời khi có một vài thiết bị hư hỏng.

3. Thuê bao mạng cáp quang phải tối thiểu có hai nhà cung cấp và kết nối vào Trường theo hai hướng tuyến khác nhau.

4. Đảm bảo các điều kiện vận hành ổn định hệ thống như điện dự phòng, hệ thống lạnh, chống sét, chống ẩm, ngập lụt, cây đổ và các hình thức thiên tai khác.

5. Hệ thống lưu điện dự phòng UPS phải có khả năng duy trì thời gian hoạt động của phòng máy chủ tối thiểu 30 phút khi mất điện, trang bị hệ thống điện dự phòng chủ động khác như nguồn phụ, máy phát điện, điện năng lượng mặt trời.

6. Trang bị đầy đủ thiết bị phòng chống cháy nổ cho phòng máy chủ và định kỳ kiểm tra tính sẵn sàng hoạt động của hệ thống phòng chống cháy nổ.

7. Có kế hoạch định kỳ kiểm tra nhằm phát hiện kịp thời các sự cố hư hỏng thiết bị của hệ thống mạng và phòng máy chủ.

Điều 19. Sao lưu dữ liệu phòng máy chủ

1. Sao lưu dữ liệu phòng máy chủ nhằm tránh hư hỏng và mất mát dữ liệu của hệ thống thông tin Nhà trường cho cả hai tình huống bị tấn công mạng và bị hư hỏng thiết bị.

2. Thực hiện sao lưu theo quy tắc 3-2-1-1-0, trong đó:

a) 3 (Bản sao dữ liệu): Giữ tổng cộng 3 bản sao: 1 bản chính đang hoạt động và 2 bản sao lưu khác.

b) 2 (Phương tiện khác nhau): Lưu trữ dữ liệu trên ít nhất 2 loại thiết bị khác nhau để tránh hỏng hóc phần cứng đồng loạt.

c) 1 (Vị trí khác): Giữ ít nhất 1 bản sao lưu ngoài phạm vi văn phòng hoặc trên điện toán đám mây để tránh rủi ro thiên tai, hỏa hoạn.

d) 1 (Không sửa đổi/ngắt kết nối): Một bản sao lưu đặc biệt không thể bị xóa, không thể sửa đổi, hoặc ngắt kết nối hoàn toàn với mạng để ngăn chặn mã hóa dữ liệu đòi tiền chuộc.

e) 0 (Không có lỗi): Thường xuyên kiểm tra và giám sát các bản sao lưu để đảm bảo không có lỗi và có khả năng phục hồi dữ liệu.

3. Đối tượng sao lưu: cơ sở dữ liệu của các phần mềm, hệ thống file dữ liệu và các máy chủ ảo.

4. Thời gian sao lưu:

a) Sao lưu toàn bộ: thực hiện tối thiểu một tuần một lần.

b) Sao lưu vi sai: thực hiện hằng ngày.

5. Đảm bảo tính bảo mật dữ liệu của các phiên bản sao lưu tương đương với bản chính thức đang hoạt động.

Điều 20. Giám sát an toàn hệ thống thông tin

1. Bố trí nhân sự chuyên trách thực hiện giám sát an toàn hệ thống thông tin.

2. Thường xuyên giám sát lưu lượng vào ra hệ thống mạng Nhà trường.

3. Hệ thống thông tin phải được kiểm tra giám sát định kỳ nhằm kịp thời phát hiện các khả năng xảy ra mất an toàn thông tin. Việc kiểm tra giám sát có thể tự thực hiện hoặc thuê dịch vụ các công ty cung cấp dịch vụ bảo mật.

4. Định kỳ sử dụng các công cụ dò quét lỗ hổng hệ thống phần mềm, điểm yếu an ninh mạng, an toàn thông tin để có thể phát hiện được các lỗ hổng bảo mật mới nhất.

5. Định kỳ tổ chức diễn tập an toàn thông tin hoặc tham gia các sự kiện diễn tập an toàn thông tin của Công an tỉnh Khánh Hòa hoặc Bộ Giáo dục và Đào tạo.

Điều 21. Ứng cứu sự cố an toàn thông tin

Khi xảy ra sự cố an toàn thông tin, cần thực hiện:

1. Đánh giá mức độ mất an toàn của sự cố để áp dụng các biện pháp xử lý phù hợp.

a) Thấp: sự cố chỉ gây ảnh hưởng cá nhân.

b) Trung bình: sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hoặc tạm dừng hoạt động chính Nhà trường.

c) Cao: sự cố tác động đến khả năng vận hành của hệ thống thông tin, ảnh hưởng đến dữ liệu, thiết bị, gây ảnh hưởng đến hoạt động chung của Nhà trường.

d) Nghiêm trọng: sự cố gây tạm dừng hoạt động của Nhà trường, gây thiệt hại nghiêm trọng đến tài sản và dữ liệu.

2. Trường hợp sự cố vượt quá khả năng xử lý, cần thông báo cho Công an tỉnh Khánh Hòa hoặc đơn vị chuyên trách về an toàn thông tin để được hướng dẫn, hỗ trợ hoặc điều phối ứng cứu xử lý sự cố.

3. Quá trình xử lý sự cố phải được ghi chép và lưu trữ hồ sơ; bảo toàn bằng chứng, chứng cứ phục vụ cho việc kiểm tra, xử lý, khắc phục và phòng ngừa sự cố cho các lần sau cũng như cung cấp chứng cứ cho cơ quan Công an khi có yêu cầu.

Chương VI
TỔ CHỨC THỰC HIỆN

Điều 22. Trách nhiệm của viên chức, người lao động và người học

1. VC, NLĐ và người học Trường Đại học Nha Trang thực hiện các quy định về an ninh mạng và an toàn thông tin cá nhân theo Quy định này và các quy định pháp luật hiện hành có liên quan.

2. Đối với từng phần mềm cụ thể, thực hiện theo Quy định về quản lý, khai thác, vận hành và phân quyền sử dụng các phần mềm quản lý của Trường.

Điều 23. Trách nhiệm của Phòng Công tác Sinh viên, Ban Biên tập website, Đoàn Thanh niên Trường

1. Tuyên truyền, phổ biến rộng rãi cho VC, NLĐ và người học nhận biết các kiến thức về an ninh mạng và an toàn thông tin cá nhân trên không gian mạng Nhà trường, các tình huống có khả năng xảy ra mất an toàn thông tin để chủ động phòng tránh.

2. Kiểm tra theo dõi không gian mạng Nhà trường, đặt biệt là các mạng xã hội, nhằm kịp thời phát hiện và đề xuất biện pháp xử lý các trường hợp vi phạm Khoản 1, 2 Điều 5 Chương II của Quy định này và Luật An ninh mạng.

Điều 24. Trách nhiệm của Phòng Hạ tầng và Công nghệ Thông tin

1. Là đơn vị chủ trì tham mưu triển khai thực hiện các nội dung về an ninh mạng và an toàn thông tin tại Trường theo Quy định này.

2. Đăng ký hồ sơ và vận hành hệ thống theo tiêu chuẩn an toàn hệ thống thông tin cấp độ 3 theo Quy định này.

3. Bố trí tối thiểu một nhân lực chuyên trách an toàn thông tin nhằm thực hiện các nhiệm vụ kiểm tra, giám sát an toàn thông tin và xử lý ứng cứu sự cố an toàn thông tin.

4. Xây dựng các quy trình ứng cứu sự cố an toàn thông tin theo các trường hợp có thể xảy ra.

5. Phối hợp với Công an tỉnh Khánh Hòa và các đơn vị chuyên trách về an toàn thông tin khi có sự cố tấn công mạng.

6. Định kỳ hằng năm đánh giá và đề xuất các nội dung cải tiến chất lượng công tác an toàn thông tin.

7. Bồi dưỡng chuyên môn định kỳ hằng năm cho nhân lực an toàn thông tin của Nhà trường.

8. Phối hợp với Khoa CNTT trong việc nghiên cứu và triển khai các giải pháp mới để nâng cao chất lượng và hiệu quả công tác an toàn thông tin.

Điều 25. Trách nhiệm của Văn phòng trường

1. Phối hợp với Phòng Hạ tầng và CNTT trong việc bảo vệ an toàn các thiết bị CNTT vật lý (dây dẫn, thiết bị mạng, thiết bị wifi,…) thuộc hệ thống mạng trong toàn Trường.

2. Sử dụng và vận hành hệ thống camera giám sát các khu vực trong Trường.

Điều 26. Xử lý vi phạm

Các tổ chức, đơn vị hoặc cá nhân vi phạm các điều khoản trong Quy định này tùy theo tính chất, mức độ sẽ bị xem xét xử lý theo quy định hiện hành của Nhà trường và cơ quan cấp trên./.