ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC SƯ PHẠM

Số: 678 /QĐ-ĐHSP

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

Thái Nguyên, ngày 31 tháng 3 năm 2023

QUYẾT ĐỊNH

Ban hành Quy định quản lý, bảo mật, an toàn thông tin và sử dụng mạng máy tính nội bộ của Trường Đại học Sư phạm - Đại học Thái Nguyên

HIỆU TRƯỞNG TRƯỜNG ĐẠI HỌC SƯ PHẠM

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

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 31/CP ngày 04 tháng 4 năm 1994 của Chính phủ về việc thành lập Đại học Thái Nguyên;

Căn cứ Thông tư số 10/2020/TT-BGDĐT ngày 14 tháng 5 năm 2020 của Bộ trưởng Bộ Giáo dục và Đào tạo về việc ban hành Quy chế tổ chức và hoạt động của Đại học vùng và các cơ sở giáo dục đại học thành viên;

Căn cứ Nghị quyết số 39/NQ-HĐĐHTN ngày 19 tháng 11 năm 2021 của Hội đồng Đại học Thái Nguyên ban hành Quy chế tổ chức và hoạt động của Đại học Thái Nguyên;

Căn cứ Nghị quyết số 40/NQ-HĐT ngày 29 tháng 12 năm 2020 của Hội đồng Trường Đại học Sư phạm ban hành Quy chế tổ chức và hoạt động của Trường Đại học Sư phạm; Nghị quyết số 54/NQ-HĐT ngày 12 tháng 12 năm 2022 của Hội đồng trường Trường Đại học Sư phạm sửa đổi, bổ sung một số điều và sửa đổi phụ lục Quy chế tổ chức và hoạt động của Trường Đại học Sư phạm ban hành kèm theo Nghị quyết số 40/NQ-HĐT ngày 29 tháng 12 năm 2020 của Hội đồng trường Trường Đại học Sư phạm;

Căn cứ Nghị định số 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng;

Căn cứ Chỉ thị số 05/2007/CT-TTg ngày 02 tháng 3 năm 2007 của Thủ tướng Chính phủ về tăng cường bảo vệ và phát huy giá trị tài liệu lưu trữ;

Theo đề nghị của Trưởng phòng Phòng Công nghệ thông tin - Thư viện.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy định về việc quản lý, bảo mật, an toàn thông tin và sử dụng mạng máy tính nội bộ của Trường Đại học Sư phạm - Đại học Thái Nguyên.

Điều 2. Quyết định này có hiệu lực kể từ ngày ký và thay thế Quyết định số 3215/QĐ-ĐHSP, ngày 10 tháng 8 năm 2018 của Hiệu trưởng Trường Đại học Sư phạm - Đại học Thái Nguyên Quy định về hoạt động quản lý và đảm bảo an toàn cho hệ thống mạng Lan và phòng máy chủ của Trường Đại học Sư phạm – Đại học Thái Nguyên.

Điều 3. Các trưởng đơn vị thuộc Trường, viên chức, người lao động và người học của Trường chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3 (để t/h);
- Website (để t/b);
- Lưu: VT, CNTT&TV (03).

HIỆU TRƯỞNG

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC SƯ PHẠM
ĐẠI HỌC THÁI NGUYÊN

PGS.TS Mai Xuân Trường

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC SƯ PHẠM

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

QUY ĐỊNH
Quản lý, bảo mật, an toàn thông tin và sử dụng mạng máy tính nội bộ của Trường Đại học Sư phạm – Đại học Thái Nguyên

(Kèm theo Quyết định số 678 /QĐ-ĐHSP ngày 31 tháng 8 năm 2023 của Hiệu trưởng Trường Đại học Sư phạm)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi, đối tượng áp dụng

1. Văn bản này quy định chi tiết về việc quản lý, bảo mật, an toàn thông tin, cơ sở dữ liệu, tài nguyên mạng và thiết bị công nghệ thông tin của Trường Đại học Sư phạm – Đại học Thái Nguyên (sau đây viết tắt là Trường).

2. Quy định này áp dụng với các đối tượng gồm: viên chức, người lao động và người học hiện đang công tác và học tập tại Trường.

Điều 2. Giải thích từ ngữ

1. Thiết bị công nghệ thông tin: Là toàn bộ các trang thiết bị phần cứng như: Máy trạm (PC, Laptop), máy chủ (Server), máy in, máy quét, máy chiếu, các loại ổ ghi đĩa CD và DVD, ổ cứng, thẻ nhớ (USB), camera số, máy ảnh số; hệ thống thiết bị mạng: thiết bị chuyển mạch (switch), tường lửa (firewall), bộ định tuyến (Router), hệ thống cáp mạng, thiết bị thu phát không dây (Access point), thiết bị lưu điện (UPS) và các thiết bị đầu cuối có kết nối mạng.

2. Cơ sở dữ liệu (Database): Là kho thông tin lưu trữ dữ liệu trên máy tính được thiết kế, tổ chức để dễ dàng quản lý và sử dụng.

3. Tài nguyên mạng: Là toàn bộ các phần mềm dùng chung chạy trên mạng nội bộ của Trường, bao gồm: Cổng thông tin của Trường và website các đơn vị, các phần mềm dùng chung của Trường (phần mềm IU, phần mềm Test online, phần mềm thi trắc nghiệm, phần mềm Đăng ký học, phần mềm Misa, phần mềm thi tiếng Anh, phần mềm LCMS/LMS, phần mềm quản trị thư viện tích hợp, Microsoft 365,…), phần mềm của Đại học Thái Nguyên (ĐHTN), phần mềm của Bộ Giáo dục và Đào tạo (BGDĐT) (nếu có), email công vụ, các phần mềm được cài đặt trên hệ thống máy tính của Trường.

4. Người sử dụng: Là viên chức, người lao động, người học của Trường sử dụng thiết bị công nghệ thông tin để khai thác mạng LAN và các tài nguyên mạng nội bộ của Trường thông qua mạng LAN, mạng Internet và kết nối mạng WAN của ĐHTN.

5. Bộ phận Quản trị mạng: Là những viên chức, người lao động thuộc Phòng Công nghệ thông tin và Thư viện (CNTT&TV) được giao nhiệm vụ quản trị hệ thống thiết bị công nghệ thông tin, duy trì sự hoạt động mạng máy tính nội bộ tại Trường; hướng dẫn sử dụng thiết bị công nghệ thông tin và khai thác tài nguyên mạng phục vụ các nhiệm vụ chuyên môn của Trường.

Chương II
QUẢN LÝ, SỬ DỤNG MẠNG MÁY TÍNH NỘI BỘ

Điều 3. Trách nhiệm của bộ phận Quản trị mạng

1. Có nhiệm vụ quản lý, vận hành hệ thống máy chủ của Trường, quản lý các máy chủ vật lý (máy chủ Domain, máy chủ DNS, máy chủ Web, máy chủ backup dữ liệu, máy chủ dịch vụ,…), hệ thống máy chủ ảo (VPS cho các ứng dụng), thiết bị mạng, hệ thống cáp mạng, thông số kỹ thuật mạng (tài khoản, mật khẩu và thông tin cấu hình của thiết bị mạng), bảo đảm hoạt động của các máy tính trên hệ thống mạng, giải quyết các sự cố liên quan. Trực tiếp theo dõi, giám sát việc sử dụng các dịch vụ mạng máy tính trong Trường (các đường truyền Internet đến các nhà mạng); cấp quyền, phân quyền truy cập và địa chỉ IP cho người sử dụng kết nối máy tính vào mạng máy tính của Trường theo đúng thông tin cấu hình chung của hệ thống.

2. Quản lý tài khoản (User, password) do Google, Microsoft cấp cho Trường, bao gồm các tài khoản: Google Admin, super Admin, groups Admin, services Admin đối với các gói dịch vụ của Google và tài khoản Admin quản lý dịch vụ Google Workspace for Education;…(Phụ lục I). Quản lý các tài khoản quản trị hệ thống (tài khoản đường truyền Internet, tài khoản Firewall, CoreSwitch, DistributionSwitch, tài khoản truy cập các máy chủ,…) (Phụ lục II).

3. Quản lý và duy trì hoạt động hệ thống mạng của Trường, đảm bảo hoạt động các dịch vụ chia sẻ dữ liệu, ứng dụng, CSDL, thư điện tử (Email), cổng thông tin điện tử (portal TNUE, Website các đơn vị), các dịch vụ trực tuyến và Intenet; Đảm bảo các hoạt động hỗ trợ kỹ thuật cho các đơn vị trong Trường; Chủ trì phối hợp với các đơn vị trong Trường thiết lập phân quyền truy cập đến các phân vùng mạng trong hệ thống mạng chung của trường để đảm bảo cho hệ thống mạng hoạt động ổn định và thông suốt.

4. Thực hiện các hoạt động duy trì, bảo dưỡng và nâng cấp cho mạng Trường bao gồm hệ thống tường lửa, định tuyến, chuyển mạch, hệ thống máy chủ, hệ thống cáp truyền dẫn, xử lý các yêu cầu về di chuyển, thay đổi thông số hệ thống mạng.

5. Kiểm tra, giám sát việc sử dụng các kết nối và các dịch vụ mạng của Trường đã cấp cho các đơn vị tham gia vào mạng. Được quyền yêu cầu các đơn vị tham gia vào mạng của Trường phải cung cấp các thông tin và các số liệu liên quan tới mạng đơn vị.

6. Trong trường hợp các đơn vị và cá nhân không tuân thủ các điều kiện đảm bảo

kỹ thuật, an toàn thông tin mạng, bộ phận Quản trị mạng sẽ gửi thông báo nhắc nhở trước khi tạm ngừng việc cung cấp dịch vụ mạng.

Điều 4. Trách nhiệm của người sử dụng khi truy cập mạng nội bộ

1. Việc truy cập vào mạng nội bộ phải xuất phát từ yêu cầu phục vụ công tác quản lý, điều hành, các nhiệm vụ mang tính chuyên môn phục vụ cho các hoạt động của Trường.

2. Khi có sự thay đổi vị trí làm việc của phòng, việc giữ nguyên hoặc thay đổi các tham số đã cài đặt trên máy tính thì các đơn vị sử dụng phải thông báo đến bộ phận Quản trị mạng để cùng phối hợp và giải quyết.

3. Người sử dụng truy cập từ xa vào tài nguyên mạng và thiết bị công nghệ thông tin trong mạng nội bộ Trường có trách nhiệm bảo mật thông tin, thông số kỹ thuật kết nối mạng. Nghiêm cấm việc cung cấp, để lộ, truyền thông tin ra bên ngoài.

4. Việc truy cập vào mạng nội bộ thông qua thiết bị wireless (wifi) trong khu vực nhà làm việc A1, A2, A3, A4, giảng đường B1, B2, B3, B4, B5, A5, Nhà thí nghiệm, Thư viện, Hội trường C1 và C2, Trường Trung học phổ thông Thái Nguyên (THPT) từ các thiết bị di động (laptop, smartphone, máy tính bảng, ...) chỉ phục vụ cho cán bộ, viên chức và người lao động trong Trường. Trong trường hợp cần phục vụ hội nghị, hội thảo thì người sử dụng phải báo bộ phận Quản trị mạng để phối hợp và đề xuất biện pháp giải quyết.

Điều 5. Trách nhiệm của người sử dụng khi chia sẻ dữ liệu nội bộ

1. Trong trường hợp người sử dụng và các đơn vị trong Trường có nhu cầu chia sẻ dữ liệu nội bộ ra hệ thống mạng ngoài (internet) phải báo cho bộ phận Quản trị mạng để phối hợp triển khai. Tùy theo mức độ yêu cầu, nhiệm vụ và mục đích chia sẻ, bộ phận Quản trị mạng sẽ lập biên bản sự việc để trình lãnh đạo Trường xem xét phê duyệt (nếu cần).

2. Việc chia sẻ dữ liệu nội bộ ra bên ngoài cần phải đảm bảo các quy định sau:

a) Không trao đổi, truyền dẫn thông tin nghiệp vụ thuộc Trường quản lý dưới bất kỳ hình thức nào ra bên ngoài khi chưa được lãnh đạo Trường phê duyệt.

b) Không trao đổi thông tin, dữ liệu làm ảnh hưởng đến an toàn bảo mật và hoạt động trên hệ thống mạng chung của Trường. Nếu phát hiện bất thường cần báo bộ phận Quản trị mạng để xác minh và ghi nhận sự việc.

c) Đối với dịch vụ internet: các đơn vị và người sử dụng phải tuân theo các quy định sử dụng dịch vụ internet do các cơ quan nhà nước có thẩm quyền ban hành.

Điều 6. Sử dụng mạng máy tính, tài khoản người dùng

1. Viên chức, người lao động và người học khi truy cập mạng máy tính trong Trường phải chịu trách nhiệm bảo đảm bí mật tài khoản được cấp (tài khoản email, tài

khoản quản lý IU, tài khoản truy cập và tác nghiệp IU, tài khoản Test online, tài khoản thi trắc nghiệm, tài khoản quản lý LCMS/LMS, tài khoản thuộc hệ thống Google, tài khoản phần mềm thi tiếng Anh, tài khoản quản lý Cổng thông tin trường, Website các đơn vị,... và các tài khoản tác nghiệp trên các phần mềm dùng chung của Trường); Các tài khoản người dùng sẽ được phân cấp, phân quyền tuỳ theo đối tượng người sử dụng để khai thác cơ sở dữ liệu và dịch vụ trên mạng; chịu trách nhiệm lưu giữ và bảo mật đối với tài khoản trên máy chủ được cấp cho đơn vị quản lý.

2. Viên chức, người lao động không được sử dụng mạng máy tính của Trường để khai thác, lưu trữ dữ liệu trò chơi, chương trình giải trí, phim, hình ảnh và các loại hình khác có nội dung không lành mạnh, đồi trụy, trái với truyền thống đạo đức, văn hóa, thuần phong mỹ tục của dân tộc.

3. Máy tính dùng chung bắt buộc phải đặt mật khẩu cho nhóm người dùng, không cung cấp mật khẩu cho người khác.

4. Người học chỉ được sử dụng mạng máy tính trong phòng máy thực hành phục vụ cho những nội dung học tập và nghiên cứu, tuân theo quy định của Nội quy phòng máy.

5. Sử dụng dịch vụ Thư điện tử

a) Hệ thống hòm thư điện tử công vụ (email công vụ) của Trường có địa chỉ: http://mail.tnue.edu.vn.

b) Người sử dụng trong Trường sẽ được cấp một tài khoản sử dụng hòm thư cá nhân theo hệ thống tên miền của Trường, phải đảm bảo bảo mật dữ liệu trong hòm thư và không được sử dụng tài khoản hòm thư để đăng ký, sử dụng dịch vụ vi phạm các quy định hiện hành của Nhà nước và đơn vị.

c) Đối với hộp thư điện tử đơn vị: Trưởng đơn vị chịu trách nhiệm quản lý hộp thư điện tử của đơn vị mình (không sử dụng cho cá nhân). Khi thành lập mới, giải thể hoặc thay đổi tên, căn cứ vào Quyết định của cấp có thẩm quyền ban hành, đơn vị có trách nhiệm thông báo thông tin cho bộ phận Quản trị mạng để thực hiện tạo lập, thay đổi hoặc hủy bỏ hộp thư điện tử của cơ quan, đơn vị.

d) Đối với hộp thư điện tử cá nhân: Trường hợp viên chức, người lao động mới tuyển dụng hoặc thay đổi vị trí công tác. Sau khi có quyết định tuyển dụng, điều động, Lãnh đạo đơn vị gửi thông báo bằng văn bản đề xuất cấp mới hoặc điều chỉnh thông tin hộp thư điện tử cho viên chức, người lao động (Phụ lục III, IV) qua Phòng CNTT-TV, bộ phận Quản trị mạng; Đối với sinh viên đầu khoá bộ phận Quản trị mạng sẽ tạo hộp thư điện tử theo danh sách tổng hợp đề xuất từ Phòng Công tác Sinh viên.

đ) Trường hợp viên chức, người lao động điều chuyển công tác hoặc nghỉ chế độ, người học sau khi tốt nghiệp. Sau khi có quyết định nghỉ hưu hoặc điều chuyển, tốt nghiệp. Phòng Hành chính Tổ chức (HCTC) gửi văn bản tới Phòng CNTT&TV để

thu hồi hộp thư điện tử cá nhân trong thời hạn 03-06 tháng, trong trường hợp không thông báo, sẽ xóa hộp thư điện tử cá nhân tối đa sau 12 tháng.

e) Kể từ lúc tạo lập hoặc lần truy cập cuối cùng, nếu sau 06 tháng các hộp thư điện tử không truy cập, Phòng CNTT&TV có quyền khóa tài khoản, sau 12 tháng sẽ bị thu hồi.

6. Căn cứ vào chức năng, nhiệm vụ, các đơn vị chịu trách nhiệm cập nhật, sử dụng và khai thác các cơ sở dữ liệu dùng chung, cơ sở dữ liệu chuyên ngành của Trường hiệu quả, đúng mục đích; tổ chức cung cấp các dịch vụ hành chính công trên môi trường mạng, sử dụng các phần mềm dùng chung theo đúng quy định.

Chương III
BẢO MẬT VÀ AN TOÀN THÔNG TIN

Điều 7. An toàn hệ thống

1. Việc bật, tắt các thiết bị mạng, máy tính, máy in,... phải thực thiện theo hướng dẫn sử dụng của thiết bị, hạn chế tối đa việc tắt đột ngột thiết bị.

2. Người trực tiếp sử dụng máy tính không được vận chuyển, di dời thiết bị công nghệ thông tin trong đơn vị mình khi chưa được lãnh đạo đơn vị đồng ý.

3. Không đặt các vật cứng đè lên hệ thống dây điện, cáp kết nối từ nút mạng đến máy tính. Người sử dụng không được tự ý cài đặt chương trình, phần mềm có khả năng chứa mã độc vào máy tính của Trường, nếu có nhu cầu phải báo cáo cho bộ phận Quản trị mạng biết và phải được sự đồng ý mới được cài đặt.

4. Không tự ý thay đổi tên máy, workgroup, domain, địa chỉ IP máy tính nếu không có sự đồng ý của bộ phận Quản trị mạng. Trường hợp lắp đặt thêm máy tính mới hoặc máy tính bị lỗi cần phải cài đặt lại hệ điều hành phải liên hệ bộ phận Quản trị mạng để được hướng dẫn cài đặt thông số máy tính người sử dụng.

5. Trước khi sao chép, di chuyển data từ các thiết bị như ổ đĩa ngoài, USB, đĩa CD, VCD, DVD hoặc data tải từ Internet… về máy tính, các cá nhân và đơn vị phải thực hiện kiểm tra, quét virus.

6. Không truy cập các trang web không biết rõ nguồn gốc. Nghiêm cấm mọi hành vi cài đặt hoặc phát tán virus vào hệ thống máy tính. Không được xâm nhập trái phép vào các máy trạm trong hệ thống của Trường, trừ trường hợp có sự thống nhất giữa hai bên.

7. Các kết nối bất thường, không thuộc lớp IP, tên truy cập theo quy định của đơn vị khi phát hiện kết nối vào mạng sẽ bị ngắt kết nối vào hệ thống mạng chung của Trường.

8. Kết thúc ngày làm việc, người sử dụng phải thoát khỏi các chương trình phần mềm, tắt máy tính đúng quy trình (trừ những trường hợp có kế hoạch hoặc văn bản đề nghị như: đang trong giai đoạn tuyển sinh, mở cổng đăng ký học…).

Điều 8. Bảo mật và an toàn dữ liệu

1. Nghiêm cấm hành vi để lộ thông tin về máy chủ, máy tính cá nhân (mật khẩu, tên truy cập máy chủ, địa chỉ IP, các tài khoản được phân quyền để khai thác và sử dụng phần mềm tác nghiệp) cho các đối tượng khác. Không tự ý chia sẻ thông tin đường truyền LAN, WAN của Trường ra bên ngoài.

2. Người sử dụng phải đổi mật khẩu cá nhân ngay sau khi nhận được tên tài khoản và mật khẩu đăng nhập do bộ phận Quản trị mạng cung cấp, khi đặt mật khẩu mới phải có tối thiểu là 8 ký tự, bao gồm: ký tự in hoa (A, B, C,...), ký tự thường (a, b, c,…) ký tự số (1, 2, 3, 4, 5, 6, 7, 8, 9, 0) và các ký tự đặc biệt ($, *,@,....). Trường hợp quên mật khẩu hoặc không đăng nhập được phải liên hệ với bộ phận Quản trị mạng để cấp mật khẩu mới; tự chịu trách nhiệm việc bảo vệ dữ liệu máy tính được giao sử dụng, kể cả tài nguyên được chia sẻ; không được xóa dữ liệu dùng chung đang được chia sẻ trong hệ thống mạng.

3. Cán bộ, viên chức, người lao động nghỉ công tác sẽ bị thu hồi tài khoản. Trong trường hợp chuyển bộ phận thì phải bàn giao thiết bị, tên truy cập, mật khẩu truy cập vào máy tính đang sử dụng cho người thay thế trong đơn vị mình. Người thay thế có trách nhiệm phối hợp với bộ phận Quản trị mạng để tiến hành thay đổi thông tin truy cập.

4. Đối với máy tính có số liệu kế toán, điểm và các số liệu quan trọng, cần phải lưu trữ dữ liệu dự phòng. Người sử dụng có trách nhiệm tự lưu trữ dự phòng dữ liệu để đảm bảo an toàn dữ liệu khi có sự cố xảy ra và quản lý dữ liệu dự phòng đó.

5. Các đơn vị được giao quản lý hệ thống thông tin phải thực hiện việc ghi nhật ký (logfile) trên các thiết bị mạng, thiết bị bảo mật, máy tính, phần mềm ứng dụng, hệ điều hành, cơ sở dữ liệu nhằm bảo đảm các sự kiện quan trọng xảy ra trên hệ thống được ghi nhận và lưu giữ. Các bản ghi nhật ký này phải được lưu trữ ít nhất 7 ngày, được bảo vệ an toàn nhằm sử dụng để phục vụ công tác kiểm tra, phân tích khi cần thiết.

Điều 9. Công tác an ninh, an toàn thông tin khi sử dụng thư điện tử

1. Không thực hiện gửi, nhận qua hệ thống thư điện tử các văn bản mật, thực hiện chế độ bảo mật theo quy định.

2. Không phát tán thư rác, chuyển tiếp thư có nội dung văn hoá đồi trụy, chống phá Nhà nước, kích động bạo lực và chiến tranh, gây chia rẽ đoàn kết.

3. Để đảm bảo an toàn, mật khẩu của hộp thư điện tử phải được đổi ngay lần đầu tiên khi người dùng đăng nhập vào hộp thư theo hướng dẫn tại khoản 2 Điều 8 của Quy định này.

4. Hạn chế việc truy cập hộp thư điện tử bằng máy tính không được đảm bảo an toàn và truy cập từ mạng Internet công cộng không tin cậy. Cảnh giác với những thư

điện tử có nội dung, nguồn gốc khả nghi, giả mạo.

5. Khi phát hiện có hiện tượng mất an ninh, an toàn thông tin trên mạng hoặc gặp sự cố về thư điện tử, các đơn vị, cá nhân cần thông báo ngay cho bộ phận quản trị hệ thống thư điện tử để kịp thời xử lý, khắc phục, sửa chữa.

Điều 10. Quản lý và vận hành hệ thống máy chủ phục vụ

1. Trách nhiệm và quyền hạn của đơn vị sử dụng máy chủ phục vụ

a) Quản lý và đưa thông tin lên Cổng/Trang thông tin điện tử của đơn vị và của Trường phải tuân thủ theo quy định của Bộ Văn hóa – Thể thao và Du lịch, Bộ Thông tin và Truyền thông, Bộ Khoa học và Công nghệ và pháp luật hiện hành.

b) Các đơn vị và cá nhân khi sử dụng dịch vụ máy chủ phục vụ không được làm phương tiện để truyền nhận các thông tin có nội dung xấu, phản động chống lại Nhà nước.

c) Đơn vị sử dụng phải tự chịu trách nhiệm và đảm bảo việc sử dụng nội dung dữ liệu của mình trên máy chủ vào những mục đích hợp pháp. Đặc biệt trong những trường hợp sau:

- Không sử dụng dịch vụ Hosting trong các ứng dụng vi phạm bản quyền phần mềm, sở hữu trí tuệ,… đồng thời có trách nhiệm kiểm soát và ngăn cấm người khác làm điều đó trên hệ thống của mình.

- Không được cố ý gửi, tạo liên kết hoặc trung chuyển bất kỳ loại dữ liệu nào mang tính bất hợp pháp, đe dọa, lừa dối, xúc phạm,… hay các hình thức bị ngăn cấm khác dưới bất cứ hình thức nào.

- Không được cố ý thực hiện các hành vi phát tán virus, thư rác, mã độc,… hoặc các hoạt động bất hợp pháp trên mạng.

- Không được sử dụng các chương trình hoặc dịch vụ có khả năng làm tắc nghẽn hoặc đình trệ hệ thống, như gây cạn kiệt tài nguyên hệ thống, làm quá tải bộ vi xử lý và bộ nhớ.

d) Đơn vị sử dụng phải có trách nhiệm bảo mật các thông tin của mình một cách an toàn như mật khẩu hay thông tin mật khác liên quan đến tài khoản của đơn vị và có trách nhiệm báo cho bộ phận Quản trị mạng khi phát hiện hình thức truy cập trái phép bằng tài khoản hoặc các sơ hở về bảo mật bao gồm việc mất, bị đánh cắp hoặc để lộ thông tin khác.

đ) Đơn vị sử dụng có trách nhiệm sao lưu bảo quản dữ liệu của mình.

e) Nếu vị phạm các quy định trên, hệ thống sẽ ngừng cung cấp dịch vụ mà không thông báo trước để đảm bảo an toàn cho hệ thống.

2. Trách nhiệm và quyền hạn của đơn vị cung cấp máy chủ phục vụ

a) Hệ thống máy chủ phục vụ của Trường do bộ phận Quản trị mạng của Phòng

CNTT&TV quản lý và vận hành đảm bảo cho Hệ thống hoạt động thông suốt, liên tục. Theo điều kiện cụ thể, đơn vị sử dụng dịch vụ có thể sử dụng máy chủ phục vụ của mình đặt tại đơn vị hoặc phòng máy chủ của Trường.

b) Bảo đảm an toàn, bảo mật thông tin theo chế độ mật; quản lý quyền truy cập của đơn vị sử dụng dịch vụ.

c) Đảm bảo hệ thống được cài đặt phần mềm có bản quyền phòng chống mã độc, thư rác,… và bảo quản dữ liệu của đơn vị sử dụng dịch vụ hệ thống.

d) Đơn vị sử dụng dịch vụ sẽ được thông báo trong vòng 12 giờ trong trường hợp sửa chữa, nâng cấp hệ thống và khi có sự cố xảy ra như hỏng thiết bị phần cứng, đường truyền,…. Các sự cố bất khả kháng khác xảy ra với hệ thống sẽ được khắc phục trong thời gian sớm nhất.

Điều 11. Sao lưu dữ liệu dự phòng

1. Đối với các đơn vị và người sử dụng

a) Khi lưu trữ, khai thác, trao đổi thông tin, dữ liệu phải bảo đảm tính toàn vẹn, tính tin cậy, tính sẵn sàng.

b) Phải có kế hoạch sao lưu dữ liệu định kỳ.

2. Đối với đơn vị được giao quản lý dữ liệu

a) Có trách nhiệm ban hành và thực hiện quy trình sao lưu dự phòng và phục hồi cho các phần mềm, dữ liệu.

b) Xây dựng danh sách các dữ liệu, phần mềm cần 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.

c) Lập kế hoạch và thực hiện sao lưu dữ liệu dự phòng hàng ngày đối với các dữ liệu quan trọng, bao gồm: cơ sở dữ liệu và các dữ liệu quan trọng được triển khai, lưu trữ (bao gồm dữ liệu phát sinh trong quá trình vận hành các phần mềm ứng dụng). Sau khi sao lưu, lưu trữ bản sao lưu bằng thiết bị lưu trữ ngoài (như: đĩa quang, ổ cứng ngoài, các thiết bị lưu trữ khác) theo quy định lưu trữ hiện hành, bảo đảm tính sẵn sàng, bảo mật và toàn vẹn nhằm đáp ứng yêu cầu phục hồi dữ liệu, khắc phục hệ thống thông tin cho hoạt động bình thường kịp thời khi có sự cố xảy ra.

d) Lưu trữ dữ liệu sao lưu ở nơi an toàn, không cùng phân vùng lưu trữ các ứng dụng và được kiểm tra thường xuyên, bảo đảm sẵn sàng cho việc sử dụng khi cần thiết (ví dụ: điện toán đám mây).

Điều 12. Xử lý sự cố

Trong quá trình sử dụng và khai thác mạng nội bộ nếu có sự cố xảy ra, các đơn vị và cá nhân phải kịp thời thông báo đến bộ phận Quản trị mạng. Trường hợp sự cố cần

phối hợp xử lý, bộ phận Quản trị mạng tiến hành lập biên bản, tìm hiểu nguyên nhân sự cố đồng thời báo cáo Lãnh đạo Trường để có giải pháp xử lý kịp thời (Phụ lục V). Trường hợp những lỗi sự cố không khắc phục được, Phòng CNTT&TV báo cáo Hiệu trưởng và đề xuất giải pháp, xử lý phù hợp.

Chương IV
KHEN THƯỞNG, KỶ LUẬT

Điều 13. Khen thưởng

Trường xem xét, quyết định khen thưởng theo chế độ chung đối với các đơn vị, cá nhân có thành tích đặc biệt trong việc quản lý, bảo mật, an toàn thông tin và sử dụng mạng nội bộ hiệu quả. Nếu có những cải tiến nâng cao năng suất thiết bị; tiết kiệm tài nguyên; phục hồi, vận hành máy móc thiết bị cũ đạt hiệu quả thiết thực thì được khen thưởng theo chế độ sáng kiến cải tiến kỹ thuật, thực hành tiết kiệm chống lãng phí.

Điều 14. Xử lý vi phạm

Mọi hành vi vi phạm, tuỳ theo tính chất, mức độ có thể bị xử lý theo quy định hiện hành của Trường; Trường hợp vị phạm mang tính chất nghiêm trọng, gây thiệt hại lớn sẽ bị xử lý hành chính hoặc bị truy cứu trách nhiệm hình sự và phải chịu trách nhiệm bồi thường vật chất về những thiệt hại gây ra theo quy định của pháp luật.

Chương V
TỔ CHỨC THỰC HIỆN VÀ HIỆU LỰC THI HÀNH

Điều 15. Tổ chức thực hiện

1. Phòng CNTT&TV chịu trách nhiệm quản lý, triển khai, theo dõi tình hình sử dụng mạng máy tính trong Trường và báo cáo Hiệu trưởng.

2. Các Trưởng đơn vị trong Trường có trách nhiệm triển khai, phổ biến Quy định tới viên chức, người lao động và người học.

3. Viên chức, người lao động và người học trong Trường có trách nhiệm thi hành Quy định này.

Điều 16. Hiệu lực thi hành

Quy định này có hiệu lực kể từ ngày ký ban hành. Các nội dung chưa được đề cập ở Quy định này được thực hiện theo quy định pháp luật hiện hành.

Trong quá trình thực hiện, nếu có phát sinh vướng mắc, các đơn vị, cá nhân có liên quan phản ánh về Trường (qua Phòng CNTT&TV) tổng hợp, báo cáo Hiệu trưởng điều chỉnh, sửa đổi, bổ sung cho phù hợp./.

Phụ lục I

LOẠI TÀI KHOẢN QUẢN TRỊ ỨNG DỤNG

(Kèm theo Quyết định số 678/QĐ-ĐHSP ngày 31 tháng 3 năm 2023 của Hiệu trưởng Trường Đại học Sư phạm)

STT	ỨNG DỤNG	ĐƠN VỊ/CÁ NHÂN	TÀI KHOẢN
1	Ứng dụng thư điện tử (Email) trên hệ thống máy chủ Google	- Phòng CNTT-TV *(Bộ phận Quản trị mạng)*	Admin
		- Viên chức, người lao động - Người học	User
2	Ứng dụng Google Workspace for Education (dùng cho giảng viên).	- Phòng CNTT-TV *(Bộ phận Quản trị mạng)*	Admin
		- Giảng viên	User
3	Microsoft Office 365	- Phòng CNTT-TV *(Bộ phận Quản trị mạng)*	Admin
		- Viên chức, người lao động - Người học	User
4	Quản lý Cổng thông tin TNUE	- Ban Biên tập *(Bộ phận thường trực KT)*	Admin
		- Viên chức, người lao động - Người học	User

Phụ lục II

LOẠI TÀI KHOẢN QUẢN TRỊ PHẦN MỀM

(Kèm theo Quyết định số 678 /QĐ-ĐHSP ngày 21 tháng 3 năm 2023 của Hiệu trưởng Trường Đại học Sư phạm)

STT	PHẦN MỀM	ĐƠN VỊ/CÁ NHÂN	TÀI KHOẢN
1	Phần mềm Quản lý đào tạo IU	- Phòng Đào tạo	Admin
		- Phòng CTSV - Phòng BĐCLGD - Phòng KH-TC - Các Khoa chuyên môn	User
2	Phần mềm hệ thống LMS/LCMS	- Phòng CNTT-TV	Admin
		- Phòng Đào tạo - Các Khoa chuyên môn - Giảng viên	User
3	Website nhập điểm	- Phòng Đào tạo	Admin
		- Các Khoa chuyên môn - Giảng viên	User
4	Website đăng ký tín chỉ	- Phòng Đào tạo	Admin
		- Giảng viên - Sinh viên	User
5	Phần mềm thi Test Online	- Phòng BĐCLGD	Admin
		- Sinh viên	User
6	Phần mềm trộn đề thi tự luận	- Phòng BĐCLGD	Admin/User
7	Phần mềm kế toán Misa	- Phòng KH-TC	Admin/User
8	Cổng thông tin TNUE - Website các phòng - Website các khoa	Phòng CNTT-TV - Các phòng - Các khoa	Admin/User Admin/User Admin/User
9	Phần mềm Thư viện số	Phòng CNTT-TV	Admin/User
		- Các phòng - Các khoa - Sinh viên	User User User
10	Hệ thống Quản lý hành chính điện tử E-Office	- Bộ Giáo dục và Đào tạo - Văn thư (HCTC)	Admin User
11	Hệ thống Quản lý hành chính I-Office	Phòng CNTT&TV - Các phòng, khoa	Admin User
12	Phần mềm Quản lý nhân sự	- Phòng Quản lý HCTC - Phòng Quản lý khoa học	Admin User
13	Phần mềm Quản lý khoa học	- Phòng Quản lý HCTC - Phòng Quản lý khoa học	Admin/User
14	Hệ thống Quản lý văn bản ĐHTN	- ĐH Thái Nguyên - Văn thư (HCTC)	Admin User
15	Phần mềm QLKH (ĐHTN)	- ĐH Thái Nguyên - VC, NLĐ	Admin User
16	Phần mềm Quản lý nhân sự (ĐHTN)	- ĐH Thái Nguyên - VC, NLĐ	Admin User
17	Trang thông tin cá nhân (Mysite ĐHTN)	- ĐH Thái Nguyên - VC, NLĐ	Admin User

Phụ lục III

MẪU ĐỀ NGHỊ VỀ VIỆC ĐIỀU CHỈNH HÒM THƯ ĐIỆN TỬ

(Kèm theo Quyết định số 678 /QĐ-ĐHSP ngày 31 tháng 3 năm 2023 của Hiệu trưởng Trường Đại học Sư phạm)

TRƯỜNG ĐẠI HỌC SƯ PHẠM
ĐƠN VỊ: ....

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

Thái Nguyên, ngày...tháng...năm 202...

ĐỀ NGHỊ
Về việc điều chỉnh hòm thư điện tử

Hiện nay ..... có sự điều chỉnh....., để viên chức/người lao động/người học trong đơn vị có thể sử dụng hòm thư điện tử theo tên miền của Nhà trường *(@tnue.edu.vn)* trong các hoạt động chuyên môn. .....kính gửi danh sách điều chỉnh trong bảng sau:

STT	HỌ VÀ TÊN	CHỨC VỤ	ĐIỆN THOẠI	GHI CHÚ
1				
2				
3				
...				

Kính đề nghị Phòng Công nghệ thông tin và Thư viện điều chỉnh hòm thư điện tử cho người dùng trong danh sách trên.

NGƯỜI LẬP BIỂU
(Ký, ghi rõ họ tên)

LÃNH ĐẠO ĐƠN VỊ
(Ký, ghi rõ họ tên)

Phụ lục IV

MẪU ĐỀ NGHỊ VỀ VIỆC CẤP MỚI HÒM THƯ ĐIỆN TỬ

(Kèm theo Quyết định số 678 /QĐ-ĐHSP ngày 31 tháng 3 năm 2023 của Hiệu trưởng Trường Đại học Sư phạm)

TRƯỜNG ĐẠI HỌC SƯ PHẠM
ĐƠN VỊ: ....

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

Thái Nguyên, ngày...tháng...năm 202....

ĐỀ NGHỊ
Về việc cấp mới hòm thư điện tử

Hiện nay ..... có sự bổ sung....., để viên chức/người lao động/người học trong đơn vị có thể sử dụng hòm thư điện tử theo tên miền của Nhà trường *(@tnue.edu.vn)* trong các hoạt động chuyên môn. .....kính gửi danh sách cấp mới trong bảng sau:

STT	HỌ VÀ TÊN	CHỨC VỤ	ĐIỆN THOẠI	GHI CHÚ
1				
2				
3				
...				

Kính đề nghị Phòng Công nghệ thông tin và Thư viện cấp mới hòm thư điện tử cho người dùng trong danh sách trên.

NGƯỜI LẬP BIỂU
(Ký, ghi rõ họ tên)

LÃNH ĐẠO ĐƠN VỊ
(Ký, ghi rõ họ tên)

Phụ lục V

MẪU BIÊN BẢN KIỂM TRA SỰ CỐ VỀ CÔNG NGHỆ THÔNG TIN

(Kèm theo Quyết định số 678 /QĐ-ĐHSP ngày 31 tháng 3 năm 2023 của Hiệu trưởng Trường Đại học Sư phạm)

TRƯỜNG ĐẠI HỌC SƯ PHẠM
PHÒNG CÔNG NGHỆ THÔNG TIN VÀ THƯ VIỆN

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

BIÊN BẢN KIỂM TRA SỰ CỐ VỀ CÔNG NGHỆ THÔNG TIN

Hôm nay, ngày…… tháng……. năm 202..

Chúng tôi gồm:

1. Ông/Bà..... Đơn vị:.....

Là người sử dụng thiết bị ..... tại.....

2. Ông/Bà..... Đơn vị: Phòng Quản trị phục vụ
3. Ông/Bà..... Đơn vị: Phòng CNTT & TV

Cùng tiến hành kiểm tra: .....

.....

Tình trạng trước khi kiểm tra: .....

.....

Sơ bộ nguyên nhân: .....

.....

Biện pháp xử lý sự cố:.....

Kết quả sau khi xử lý:.....

Hoạt động tốt ☐ Hoạt động tạm thời ☐ Không hoạt động được ☐

Nguyên nhân: .....

.....

.....

Đề nghị: .....

.....

Thái Nguyên, ngày……tháng….năm 202…

Người sử dụng ***Phòng Quản lý CSVC*** ***Phòng CNTT& TV***