PHÒNG GDĐT TP THỦ DẦU MỘT  **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**

**TRƯỜNG TIỂU HỌC PHÚ THỌ Độc lập – Tự do – Hạnh phúc**

 Số: 24/QĐ-THPT *Phú Thọ, ngày 03 tháng 6 năm 2021*

**QUYẾT ĐỊNH**

**Ban hành Quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động**

 **ứng dụng công nghệ thông tin của Trường Tiểu học Phú Thọ**

**HIỆU TRƯỞNG TRƯỜNG TIỂU HỌC PHÚ THỌ**

*Căn cứ nhiệm vụ và quyền hạn của Hiệu trưởng quy định tại Điểm d Khoản 1 Điều 11 Chương 2 Điều lệ Trường tiểu học được ban hành kèm theo Thông tư số 28/2020/TT-BGDĐT ngày 04/9/2020 của Bộ trưởng Bộ Giáo dục và Đào tạo;*

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

 *Căn cứ Luật An ninh mạng ngày 01 tháng 01 năm 2019;*

 *Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động cơ quan nhà nước;*

 *Công văn số 1881/UBND-TH ngày 01/8/2014 của UBND thành phố Thủ Dầu Một về việc quy định bảo mật thông tin trong hoạt động cơ quan nhà nước;*

*Công văn số 490/QĐ-PGDĐT ngày 07/4/2020 của Phòng Giáo dục và Đào tạo thành phố Thủ Dầu Một Quyết định Ban hành Quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Ngành Giáo dục và Đào tạo Thành phố Thủ Dầu Một;*

 Xét đề nghị của bộ phận chuyên môn.

**QUYẾT ĐỊNH:**

 **Điều 1.** Ban hành kèm theo Quyết định này “Quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Trường Tiểu học Phú Thọ”.

 **Điều 2.** Quyết định này có hiệu lực kể từ ngày ký.

 **Điều 3.** Cán bộ, giáo viên, nhân viên Trường Tiểu học Phú Thọ chịu trách nhiệm thi hành quyết định này./.

***Nơi nhận:*** **HIỆU TRƯỞNG**

- VC, NV ((website);

- HT;

- Lưu: VT.

 **Nguyễn Thị Thanh Tâm**

**QUY CHẾ**

 **Về bảo đảm an toàn, an ninh thông tin trong hoạt động**

**ứng dụng công nghệ thông tin của Trường Tiểu học Phú Thọ**

*(Ban hành kèm theo Quyết định số 24/QĐ-THPT ngày 03 tháng 6 năm 2021*

*của Trường Tiểu học Phú Thọ)*

**Chương I**

**QUY ĐỊNH CHUNG**

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

1. Quy chế này áp dụng về công tác bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Trường Tiểu học Phú Thọ (sau đây gọi tắt là đơn vị).

2. Quy chế này được áp dụng với các tổ chức, cá nhân liên quan đến an toàn, an ninh thông tin của đơn vị.

**Điều 2. Mục đích, nguyên tắc đảm bảo an toàn thông tin**

1. Việc áp dụng Quy chế này nhằm giảm thiểu được các nguy cơ gây mất an toàn thông tin và đảm bảo an ninh thông tin trong quá trình ứng dụng công nghệ thông tin trong hoạt động của các đơn vị.

2. Các hoạt động ứng dụng công nghệ thông tin phải tuân theo nguyên tắc đảm bảo an toàn thông tin được quy định tại điều 41, Nghị định 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước.

**Chương II**

**QUY ĐỊNH ĐẢM BẢO AN TOÀN THÔNG TIN**

 **Điều 3. Về quản lý viên chức và người lao động**

1. Đơn vị xây dựng các yêu cầu, trách nhiệm đảm bảo an toàn thông tin đối với từng vị trí công việc. Trước khi tiếp nhận nhân sự, đơn vị phải kiểm tra khả năng đáp ứng các yêu cầu và an toàn thông tin của nhân sự mới.

2. Đơn vị thường xuyên tổ chức quán triệt các quy định về an toàn thông tin, nhằm nâng cao nhận thức về trách nhiệm đảm bảo an toàn thông tin của từng cá nhân trong đơn vị.

3. Giao cho giáo viên Tin học thu hồi quyền truy cập các hệ thống thông tin, các tài sản liên quan tới hệ thống thông tin đối với các cá nhân nghỉ việc, chuyển công tác.

**Điều 4. Quản lý phòng máy chủ**

1. Tùy quy mô và điều kiện, đơn vị có thể xây dựng phòng máy chủ, trong đó, các thiết bị mạng quan trọng như tường lửa (firewall), thiết bị định tuyến (router), hệ thống máy chủ, hệ thống camera,… được đặt trong phòng máy chủ và các biện pháp bảo vệ, ngăn chặn xâm nhập trái phép vào phòng máy chủ.

2. Vị trí máy chủ, thiết bị lưu trữ dữ liệu là khu vực hạn chế tiếp cận. (Không đặt máy chủ, thiết bị lưu trữ dữ liệu, hình ảnh camera,… tại phòng bảo vệ hoặc các phòng chức năng không đảm bảo an toàn). Phòng máy chủ của đơn vị là khu vực hạn chế tiếp cận và được lắp đặt hệ thống camera giám sát. Chỉ những người có trách nhiệm theo quy định của Hiệu trưởng đơn vị mới được phép vào phòng máy chủ.

3. Quá trình vào, ra phòng máy chủ phải được ghi nhận vào nhật ký quản lý phòng máy chủ.

4. Phòng máy chủ có hệ thống lưu điện đủ công suất và duy trì thời gian hoạt động của các máy chủ tối thiểu 15 phút khi có sự cố mất điện.

**Điều 5. Phòng chống mã độc**

1. Tất cả các máy trạm, máy chủ được trang bị phần mềm chống mã độc. Các phần mềm phòng chống mã độc được thiết lập chế độ tự cập nhật; chế độ tự quét mã độc khi sao chép, mở các tập tin.

2. Các viên chức và người lao động trong đơn vị về phòng chống mã độc, các rủi ro do mã độc gây ra; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm trên máy trạm khi chưa có sự đồng ý của người có thẩm quyền theo quy định của đơn vị.

3. Tất cả các máy tính của đơn vị được cấu hình nhằm vô hiệu hóa tính năng tự động thực thi (autoplay) các tập tin trên các thiết bị lưu trữ di động.

4. Tất cả các tập tin thư mục được quét mã độc trước khi sao chép, sử dụng.

5. Khi phát hiện ra bất kì dấu hiệu nào liên quan đến việc nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu,…), người sử dụng phải tắt máy và báo trực tiếp cho bộ phận có trách nhiệm để xử lý.

**Điều 6. Sao lưu dữ liệu phòng**

1. Các dữ liệu quan trọng của đơn vị phải được sao lưu, bao gồm: thông tin cấu hình của hệ thống mạng, máy chủ; phần mềm ứng dụng và cơ sở dữ liệu; tập tin ghi nhật ký.

2. Giáo viên Tin học phải lập kế hoạch, hướng dẫn các bộ phận và thực hiện sao lưu dữ liệu phù hợp với điều kiện của đơn vị, đảm bảo khả năng phục hồi dữ liệu khi có sự cố xảy ra.

**Điều 7. Quản lý thiết bị tường lửa**

1. Các hạ tầng công nghệ thông tin phải được trang bị tường lửa để ngăn chặn và phát hiện các xâm nhập trái phép vào mạng nội bộ.

2. Nhật ký hoạt động của thiết bị tường lửa phải được lưu giữ an toàn để phục vụ công tác khảo sát, điều tra khi có sự cố xảy ra.

**Điều 8. Quản lý nhật ký trong quá trình vận hành các hệ thống thông tin**

1. Giáo viên Tin học phải thực hiện việc ghi nhật ký (log) trên các thiết bị mạng máy tính, phần mềm ứng dụng, điều hành, cơ sở dữ liệu nhằm đảm bảo sự kiện quan trọng xảy ra trên hệ thống ghi nhận và lưu trữ.

2. Các nhật ký này phải được bảo vệ an toàn nhằm phục vụ công tác kiểm tra, phân tích khi cần thiết.

3. Các sự kiện tối thiểu cần phải được ghi nhật ký gồm: quá trình đăng nhập hệ thống; tạo, cập nhật hoặc xóa dữ liệu; các hành vi xem, thiết lập cấu hình hệ thống; việc thiết lập các kết nối bất thường vào ra hệ thống; thay đổi quyền truy cập hệ thống.

 4. Thường xuyên thực hiện việc theo dõi bản ghi nhật ký của hệ thống và sự kiện khác có liên quan để báo cáo đánh giá, báo cáo các rủi ro và mức độ nghiêm trọng các rủi ro đó.

**Điều 9. Quản lý truy cập**

1. Các quy định về quản lý truy cập vào hệ thống thông tin, mạng máy tính, thiết bị, phần mềm ứng dụng của đơn vị phải được quy định chi tiết và tổ chức thực hiện nghiêm túc, phù hợp với các quy định của pháp luật về an toàn thông tin.

2. Mỗi tài khoản truy cập các hệ thống thông tin chỉ được cấp cho một người quản lý và sử dụng.

3. Mỗi viên chức và người lao động chỉ được phép truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình, có trách nhiệm bảo mật tài khoản truy cập thông tin.

4. Các hệ thống thông tin cần giới hạn số lần đăng nhập vào sai liên tiếp vào hệ thống. Hệ thống tự động khóa tài khoản trong một khoảng thời gian nhất định trước khi tiếp tục cho đăng nhập nếu liên tục đăng nhập sai vượt quá số lần quy định.

5. Tất cả máy trạm, máy chủ phải được đặt mật khẩu truy cập và thiết lập chế độ tự bảo vệ màn hình sau 10 phút không sử dụng.

6. Khi thiết lập mạng không dây trong nội bộ đơn vị, phải đặt mật khẩu truy cập vào mạng không dây và chỉ cho truy cập Internet.

7. Cán bộ phụ trách hệ thống thông tin chịu trách nhiệm đảm bảo an toàn, an ninh thông tin.

8. Thay đổi mật khẩu khi tiếp nhận các hệ thống thông tin (cả camera quan sát), không sử dụng mật khẩu mặc định hoặc các mật khẩu đơn giản (VD: 123456, 123456789, abcd1234,…). Mật khẩu đăng nhập vào các hệ thống thông tin phải có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký hiệu HOA, có ký hiệu thường, ký tự số và ký tự đặc biệt như !,@, #, $, %,…) và phải được thay đổi ít nhất 3 tháng/ lần.

**Điều 10. Quản lý sự cố**

1. Phân loại mức độ nghiêm trọng của các sự cố, bao gồm:

a) Thấp: sự cố gây ảnh hưởng cá nhân và làm gián đoạn hay đình trệ hoạt động chính của đơn vị;

b) Trung bình: sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của đơn vị;

c) Cao: sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến một trong các hoạt động chính của đơn vị ;

d) Khẩn cấp: sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của đơn vị.

2. Khi có sự cố hoặc nguy cơ mất an toàn thông tin thì Hiệu trưởng đơn vị chỉ đạo giáo viên Tin học phải kịp thời để khắc phục và hạn chế thiệt hại, báo cáo bằng văn bản cho cơ quan cấp trên.

3. Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của đơn vị, Hiệu trưởng phải báo cáo ngay cho cơ quan cấp trên quản lý để được hướng dẫn, hỗ trợ.

**Điều 11. Các hành vi bị nghiêm cấm**

1. Tạo ra, cài đặt, phát tán vi rút máy tính, phần mềm độc hại trái pháp luật.

2. Xâm nhập, sửa đổi, xóa bỏ nội dung thông tin của đơn vị, cá nhân khác.

3. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin ngành.

4. Ngăn chặn việc truy cập đến thông tin của đơn vị, cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

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

6. Hành vi khác làm mất an toàn, bí mật thông tin của đơn vị, cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

7. Không được đăng tải thông tin sai sự thật gây hoang mang dư luận.

8. Không được đăng tải thông tin dâm ô, đồi trụy.

9. Không được đăng tải, phát tán thông tin tuyên truyền chống nhà nước.

10. Không được đăng tải thông tin gây rối trật tự công cộng.

1. Không được đăng tải, phát tán thông tin vu khống người khác.
2. Không được đăng tải, phát tán thông tin sai sự thật về sản phẩm, hàng hóa.
3. Không được đăng tải bí mật công tác, bí mật nhà nước.
4. Không được đăng tải thông tin phiến diện một chiều.
5. Không được giới thiệu tên, đăng tải hình ảnh đơn vị công an.

16. Nghiêm cấm các hành vi sử dụng hệ thống sai mục đích, gây nguy cơ nhiễm vi rút, phần mềm độc hại,…

17. Không sử dụng thông tin của đơn vị sai mục đích, không cung cấp thông tin đơn vị (tài khoản, thông tin học sinh, thông tin phụ huynh, thông tin nhân sự, dữ liệu, hình ảnh camera,…) cho các đối tượng, đơn vị khác, không phải Ngành Giáo dục và Đào tạo Thành phố triển khai, hướng dẫn.

**Chương III**

**TRÁCH NHIỆM ĐẢM BẢO AN TOÀN THÔNG TIN**

**Điều 12. Trách nhiệm của viên chức và người lao động trong đơn vị**

1. Trách nhiệm của viên chức phụ trách an toàn thông tin:

a) Chịu trách nhiệm đảm bảo an toàn thông tin của đơn vị;

b) Tham mưu Hiệu trưởng ban hành các quy định, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin; Tham mưu hiệu trưởng các giải pháp bảo mật hệ thống. Giám sát, đánh giá, báo cáo hiệu trưởng các rủi ro có thể xảy ra trong quá trình vận hành hệ thống.

c) Thực hiện việc giám sát, đánh giá, báo cáo Hiệu trưởng các rủi ro mất an toàn thông tin và mức độ nghiêm trọng của các rủi ro đó;

d) Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn, an ninh thông tin; tích cực, khắc phục khi xảy ra sự cố an toàn, an ninh thông tin.

e) Các dữ liệu quan trọng của đơn vị phải được sao lưu, bao gồm: thông tin cấu hình hệ thống, cơ sở dữ liệu, nhật ký hệ thống. Đảm bảo khả năng phục hồi dữ liệu khi sự cố xảy ra.

f) Tài khoản quản trị có quyền cao nhất (Admin) chỉ được cấp bằng văn bản cho một người. Các tài khoản khác khi truy cập hệ thống cần được phân quyền cụ thể, chỉ được phép truy cập các thông tin phù hợp với chức năng, nhiệm vụ, quyền hạn được phân công.

g) Người được giao tài khoản trên hệ thống có trách nhiệm bảo mật tài khoản và chịu trách nhiệm trước hiệu trưởng nếu xảy ra sự cố mất an ninh, an toàn thông tin.

h) Hệ thống mạng không dây của đơn vị phải có mật khẩu truy cập và chỉ cho phép truy cập Internet (chặn các kết nối đến hệ thống máy chủ, hệ thống mạng của đơn vị).

2. Trách nhiệm của viên chức, nhân viên trong đơn vị:

a) Nghiêm túc chấp hành các quy định, quy trình nội bộ, Quy chế này và các quy định khác của pháp luật về an toàn thông tin. Chịu trách nhiệm bảo đảm an toàn thông tin mạng phạm vi trách nhiệm và quyền hạn được giao;

b) Mỗi viên chức và người lao động phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp các thiết bị trên máy tính; không được vào các trang web không rõ về nội dung; không tải và cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến chuyên môn; không nhấp chuột vào các đường dẫn lạ không rõ về nội dung;

c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin phải báo cáo ngay với cấp trên và bộ phận chuyên trách công nghệ thông tin của đơn vị để kịp thời ngăn chặn và xử lý;

d) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin do các đơn vị có chức năng tổ chức.

**Điều 13. Trách nhiệm của Hiệu trưởng đơn vị**

1. Hiệu trưởng có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này và chịu trách nhiệm trước cấp trên và trước Ủy ban nhân dân thành phố trong công tác đảm bảo an toàn thông tin của đơn vị mình.

2. Phân công một bộ phận hoặc cán bộ chuyên môn chuyên trách đảm bảo an toàn thông tin của đơn vị; tạo điều kiện để các cán bộ phụ trách an toàn thông tin được học tập, nâng cao trình độ về an toàn thông tin.

3. Xây dựng quy định, quy trình nội bộ về đảm bảo an toàn thông tin phù hợp với Quy chế này và các quy định của pháp luật.

4. Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả.

5. Phối hợp chặt chẽ với Công an thành phố trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn, an ninh thông tin.

6. Đảm bảo an toàn, an ninh hệ thống CNTT, Hiệu trưởng quán triệt toàn thể viên chức, nhân viên thực hiện đúng theo quyết định số 490/QĐ-PGDĐT ngày 07 tháng 4 năm 2020, Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng CNTT của Ngành đến hội đồng giáo viên, viên chức của đơn vị trong đó đặc biệt quan tâm đên yếu tố “Thái độ người dùng”; Đảm bảo việc phân công trách nhiệm của cán bộ, giáo viên và viên chức CNTT khi tham gia hệ thống thông tin của ngành.

7. Nếu xảy ra sự cố mất an toàn thông tin, an ninh; đơn vị xử lý theo quy trình cụ thể.

- Thông tin mà không xử lý được, đơn vị sẽ theo quy trình xử lý sau:

- Bước 1: Báo cáo hiện trạng sự cố cho Phòng Giáo dục và Đào tạo.

- Bước 2: Phối hợp giữa các đơn vị để ngăn chặn sự cố xảy ra trong thời gian sớm nhất. Tích cực ngăn chặn sự cố, khôi phục hậu quả, đảm bảo hệ thống hoạt động ổn định, không gây ảnh hưởng đến hoạt động chung của đơn vị.

- Bước 3: Báo cáo tổng hợp thông tin về Phòng Giáo dục và Đào tạo

Đề nghị tất cả viên chức, nhân viên đơn vị nghiêm túc đảm bảo an toàn, an ninh thông tin các hệ thống CNTT của trường, của ngành.

Định kỳ hằng quý đơn vị lập báo cáo về tình hình an ninh, an toàn thông tin và gửi về Phòng Giáo dục và Đào tạo./.