UBND TP THỦ DẦU MỘT
PHÒNG GIÁO DỤC VÀ ĐÀO TẠO

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

Số: 495 /PGDĐT
V/v đảm bảo an toàn, an ninh các hệ thống CNTT tại các đơn vị trường, cơ sở giáo dục trên địa bàn thành phố

Thủ Dầu Một, ngày 07 tháng 4 năm 2020

Kính gửi:
- Hiệu trưởng các trường Mầm non, Mẫu giáo, Tiểu học, Trung học cơ sở công lập;
- Hiệu trưởng, chủ cơ sở giáo dục ngoài công lập.

Căn cứ quyết định số 490/QĐ-PGDĐT ngày 07 tháng 4 năm 2020 của Trưởng phòng Giáo dục và Đào tạo về phê duyệt Quy chế đảm bảo 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.

Nhằm nâng cao hiệu quả việc đảm bảo an toàn, an ninh các hệ thống Công nghệ thông tin (CNTT) của Ngành Giáo dục và Đào tạo, Phòng Giáo dục và Đào tạo đề nghị hiệu trưởng các đơn vị thực hiện và triển khai các giải pháp, nhiệm vụ cụ thể như sau:

I. Nội dung thực hiện:

Hiệu trưởng các đơn vị tổ chức tổng rà soát việc đảm bảo an toàn, an ninh các hệ thống thông tin của đơn vị ở những nội dung sau:

1. Tổ chức thực hiện:

1.1.Trách nhiệm của Hiệu trưởng đơn vị:

– Hiệu trưởng đơn vị có trách nhiệm tổ chức thực hiện các quy định tại Quy chế đảm bảo an toàn, an ninh thông tin.

– Ban hành quyết định phân công bộ phận hoặc cán bộ phụ trách các hệ thống của đơn vị.

– Chịu trách nhiệm trước Lãnh đạo Phòng Giáo dục và Đào tạo và Ủy ban nhân dân Thành phố trong công tác đảm bảo an toàn thông tin của đơn vị.

1.2.Trách nhiệm của cán bộ phụ trách hệ thống:

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

– Phải thay đổi mật khẩu khi tiếp nhận các hệ thống thông tin (bao gồm cả hệ thống camera quan sát), không sử dụng mật khẩu mặc định hoặc các mật khẩu đơn giản (ví dụ: 123456, 123456789, abcd1234,…). Mật khẩu phải có độ phức tạp cao

(dài tối thiểu 8 ký tự, có ký tự Hoa, ký tự thường, ký tự số, ký tự đặc biệt như: !@#$%...) và phải thường xuyên thay đổi mật khẩu.

– 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.

– Phối hợp với các cá nhân, đơn vị liên quan tích cực, khắc phục khi xảy ra sự cố an toàn, an ninh thông tin.

2. Quản trị hệ thống

2.1 Quản lý phòng máy chủ, nơi đặt thiết bị lưu trữ:

– 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).

– Chỉ những người có trách nhiệm theo sự phân công của hiệu trưởng mới được phép vào các khu vực này.

2.2 Sao lưu dữ liệu:

– 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.

2.3 Quản lý truy cập:

– 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.

– 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.

– 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).

3. Các hành vi bị cấm:

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

– 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 học sinh, 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.

4. Tuyên truyền về công tác đảm bảo an toàn, an ninh hệ thống CNTT

Nhằm nâng cao hiệu quả công tác đảm bảo an toàn, an ninh hệ thống CNTT Ngành Giáo dục và Đào tạo Thành phố. Hiệu trưởng các đơn vị cần quán triệt các nội dung theo quyết định số /QĐ-PGDĐT ngày tháng 4 năm 2020 của Trưởng phòng Giáo dục và Đào tạo về phê duyệt Quy chế đảm bảo 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 đến hội đồng giáo viên, viên chức của đơn vị trong đó đặc biệt quan tâm đến yếu tố "Thái độ người dùng"; Đảm bảo việc phân công trách nhiệm của cán bộ, giáo viên và viên chức công nghệ thông tin khi tham gia hệ thống thông tin của ngành.

II. Quản lý sự cố:

Trong quá trình thực hiện nếu xảy ra sự cố mất an toàn thông tin, an ninh hệ thống thông tin đề nghị các đơn vị xữ lý theo quy trình cụ thể như sau:

Nếu phát hiện sự cố an toàn thông tin mà không xữ lý được, các đơn vị cần thực hiện theo quy trình xữ lý sau:

- Bước 1: Báo cáo hiện trạng sự cố cho Phòng Giáo dục và Đào tạo
  + Phòng Giáo dục và Đào tạo, điện thoại: 02743837298; E-mail: thudaumot@sgdbinhduong.edu.vn
  + Ông Lê Minh Tiến – Chuyên viên, điện thoại: 0913860438; E-mail: leminhtien@tptdm.edu.vn
- 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 khắc 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.

Đảm bảo an toàn, an ninh thông tin là nhiệm vụ quan trọng, ảnh hưởng trực tiếp đến việc thực hiện các nhiệm vụ chính trị, chuyên môn của đơn vị và ngành. Vì vậy Phòng Giáo dục và Đào tạo đề nghị hiệu trưởng các đơn vị nghiêm túc triển khai thực hiện các quy định về đảm bảo an toàn, an ninh thông tin các hệ thống CNTT của ngành Giáo dục và Đào tạo Thành phố./.

Nơi nhận:
- Như trên;
- Lãnh đạo Phòng GDĐT;
- Chuyên viên Phòng GDĐT;
- Website Phòng GDĐT;
- Lưu: VT, CM,TCCB.

TRƯỞNG PHÒNG

THỦ DẦU MỘT
BÌNH DƯƠNG

Người ký: Nguyễn Văn Chệt
Email: chetnv@binhduong.gov.vn
Cơ quan: Thành phố Thủ Dầu Một, Tỉnh Bình Dương
Chức vụ: Trưởng phòng Giáo dục và Đào tạo
Thời gian ký: 07.04.2020 16:41:15 +07:00