

Số: /SGDDT-VP
V/v tăng cường bảo đảm an toàn,
an ninh mạng tại các cơ sở giáo dục

Hải Phòng, ngày tháng 8 năm 2025

Kính gửi:

- Các phòng chuyên môn, nghiệp vụ thuộc Sở;
- UBND các xã, phường, đặc khu;
- Hiệu trưởng trường THPT, Phổ thông nhiều cấp;
- Thủ trưởng các đơn vị trực thuộc.

Thực hiện Công văn số 1670/CAHP ngày 28/8/2025 của Công an thành phố Hải Phòng về việc tăng cường công tác bảo đảm an toàn thông tin, an ninh mạng trên địa bàn thành phố; nhằm phòng ngừa nguy cơ tấn công mạng, lộ lọt dữ liệu, gián đoạn hệ thống thông tin của ngành giáo dục, đồng thời góp phần giữ vững an toàn thông tin trong các dịp lễ, sự kiện chính trị, xã hội quan trọng của thành phố, Sở Giáo dục và Đào tạo đề nghị các cơ sở giáo dục trên địa bàn thành phố triển khai một số nội dung sau:

1. Tăng cường công tác tuyên truyền, giáo dục

Tăng cường tuyên truyền, nâng cao nhận thức cho cán bộ, giáo viên, nhân viên, học sinh về trách nhiệm bảo đảm an toàn thông tin trên không gian mạng; nâng cao tinh thần cảnh giác trước các thủ đoạn lợi dụng mạng xã hội để phát tán thông tin xấu độc, lôi kéo, kích động.

2. Bảo đảm an toàn hệ thống công nghệ thông tin

- Thường xuyên theo dõi, giám sát hoạt động hệ thống thông tin của đơn vị. Quản lý chặt chẽ hệ thống email, website, cổng thông tin điện tử, phần mềm quản lý học sinh, học bạ điện tử, học liệu số,... kịp thời phát hiện các dấu hiệu bất thường, tấn công mạng, mã độc, không để xảy ra tình trạng mất dữ liệu hoặc bị lợi dụng phát tán thông tin sai lệch.

3. Triển khai các biện pháp bảo mật, phòng ngừa sự cố

- Rà soát, gỡ bỏ các dịch vụ không cần thiết.
- Chủ động sao lưu dữ liệu, rà soát lỗ hổng, vá lỗi kịp thời, bảo đảm hệ thống vận hành ổn định, thông suốt.
- Kiểm tra tài khoản quản trị, thay đổi mật khẩu định kỳ, áp dụng xác thực hai yếu tố để tăng cường bảo mật.
- Cập nhật các rule trên firewall (tường lửa), kiểm tra định kỳ và backup dữ liệu thường xuyên.

- Hạn chế tối đa truy cập từ xa, phân quyền người dùng hợp lý, kiểm soát chặt chẽ việc cài đặt, sử dụng phần mềm.

- Đối với các màn hình LED, LCD, pano số, áp phích điện tử: kiểm soát nội dung tuyên truyền; đổi mật khẩu truy cập thiết bị, ngắt các kết nối không cần thiết (wifi, NFC, Bluetooth); kiểm tra các Port điều khiển từ xa qua internet có bị mở hay không (3389,8080); kiểm tra thiết bị xem có bị kết nối từ xa qua VNC, AnyDesk, Teamviewer, Ultraview, RemoteDesktop, Seecreen...; tắt quyền truy cập từ xa nếu thấy không cần thiết.

4. Phối hợp, xử lý tình huống

Chủ động phối hợp chặt chẽ với công an địa phương và các cơ quan chức năng trong công tác bảo đảm an ninh mạng. Khi phát hiện sự cố an toàn thông tin mạng, hành vi lôi kéo, dụ dỗ học sinh qua mạng các đơn vị báo cáo ngay về Sở GD&ĐT (qua Văn phòng Sở), liên hệ với Công an thành phố (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, đồng chí Đại úy Lê Bảo Trung, số điện thoại: 0963368988) hoặc công an nơi gần nhất để được hướng dẫn xử lý kịp thời.

Kính đề nghị Ủy ban nhân dân các xã, phường, đặc khu quan tâm phối hợp chỉ đạo tới các cơ sở giáo dục trên địa bàn quản lý; thủ trưởng các cơ sở giáo dục nghiêm túc triển khai thực hiện nhằm bảo đảm an toàn, an ninh mạng cho các hoạt động của nhà trường và các sự kiện chính trị, xã hội quan trọng, các ngày lễ lớn của đất nước./.

Nơi nhận:

- Như trên;
- Công an thành phố (để p/h);
- Lãnh đạo Sở;
- Lưu: VT,VP.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Uông Minh Long