

Số: /SGDDĐT-VP  
V/v Nâng cao hiệu quả công tác bảo vệ  
bí mật nhà nước và an ninh mạng

Hung Yên, ngày tháng 4 năm 2026

Kính gửi:

- Ủy ban nhân dân các xã, phường;
- Các đơn vị trực thuộc Sở GDĐT;

Thực hiện Công văn số 1478/UBND-NC ngày 24/3/2026 của Ủy ban nhân dân tỉnh Hưng Yên về việc nâng cao hiệu quả công tác bảo vệ bí mật nhà nước và an ninh mạng trên địa bàn tỉnh;

Qua công tác thanh tra chuyên đề của Bộ Công an cho thấy việc chấp hành các quy định pháp luật về bảo vệ bí mật nhà nước (BMNN) và an ninh mạng tại một số cơ quan, đơn vị vẫn còn những tồn tại, hạn chế. Để khắc phục triệt để tình trạng trên và bảo đảm an toàn thông tin, an ninh dữ liệu trong toàn ngành, Sở Giáo dục và Đào tạo (GDĐT) yêu cầu thủ trưởng các đơn vị thuộc và trực thuộc Sở, đề nghị UBND xã/phường phối hợp chỉ đạo các cơ sở cơ sở giáo dục thuộc phạm vi quản lý khẩn trương thực hiện nghiêm túc các nội dung sau:

### **1. Công tác quán triệt, tuyên truyền nâng cao nhận thức và chấp hành quy định về Bảo vệ bí mật nhà nước**

- Tổ chức quán triệt, phổ biến sâu rộng đến toàn thể cán bộ, công chức, viên chức, người lao động Luật Bảo vệ bí mật nhà nước, Luật An ninh mạng và các văn bản hướng dẫn thi hành.

- Thực hiện nghiêm túc Quyết định số 57/QĐ-SGDĐT ngày 16/01/2026 của Sở GDĐT về việc ban hành Nội quy Bảo vệ bí mật nhà nước của Sở Giáo dục và Đào tạo Hưng Yên.

- Thực hiện nghiêm nguyên tắc: Tuyệt đối không kết nối Internet đối với máy tính dùng để soạn thảo, lưu trữ tài liệu chứa bí mật nhà nước (như đề thi, hồ sơ mật,...). Quản lý chặt chẽ việc sử dụng thiết bị ngoại vi (USB, ổ cứng ngoài) kết nối vào các máy tính này để phòng ngừa mã độc và nguy cơ lộ, mất BMNN.

### **2. Triển khai các biện pháp bảo đảm an ninh mạng, an toàn hệ thống thông tin**

- Thường xuyên rà soát, đánh giá các hệ thống thông tin, công thông tin điện tử, cơ sở dữ liệu của đơn vị. Triển khai các giải pháp kỹ thuật áp dụng Tiêu chuẩn quốc gia TCVN 11930:2017 và TCVN 14423:2025, đặc biệt chú trọng việc quản lý rủi ro an ninh mạng.

- Bắt buộc cài đặt phần mềm phòng, chống mã độc có bản quyền (như VNPT Smart IR,...) cho 100% máy tính công vụ và máy tính cá nhân sử dụng trong công việc để loại bỏ mã độc, khắc phục các lỗ hổng bảo mật.

- Chấn chỉnh công tác bảo mật tài khoản: Yêu cầu toàn bộ cán bộ, giáo viên thay đổi ngay "mật khẩu mặc định", sử dụng mật khẩu mạnh đối với các tài khoản truy cập Hệ thống Cơ sở dữ liệu ngành, phần mềm Quản lý văn bản và Điều hành, Học bạ số; tuyệt đối không chia sẻ tài khoản cho người khác.

### **3. Công tác kiểm tra và ứng phó sự cố**

- Người đứng đầu cơ quan, đơn vị chịu hoàn toàn trách nhiệm trước thủ trưởng đơn vị chủ quản cấp trên và trước pháp luật nếu để xảy ra sự cố mất an toàn thông tin, lộ lọt dữ liệu do nguyên nhân chủ quan, thiếu trách nhiệm hoặc không tuân thủ quy định.

- Phối hợp chặt chẽ với Đội ứng cứu sự cố an toàn thông tin mạng ngành GDĐT (đã được thành lập theo Quyết định số 1211/QĐ-SGDĐT) và Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (Công an tỉnh) để theo dõi, giám sát. Khi phát hiện nguy cơ hoặc xảy ra sự cố tấn công mạng, lộ lọt dữ liệu, phải kịp thời báo cáo để được hướng dẫn, xử lý.

Sở GDĐT yêu cầu thủ trưởng các đơn vị thuộc Sở, các đơn vị trực thuộc Sở nghiêm túc triển khai thực hiện, đề nghị UBND xã/phường phối hợp chỉ đạo, triển khai thực hiện tại các cơ sở giáo dục thuộc phạm vi quản lý. Quá trình thực hiện nếu có vướng mắc, đề nghị phản ánh về Sở GDĐT (qua Văn phòng Sở, đầu mối Đ/c Trần Văn Dũng) để tổng hợp, hướng dẫn giải quyết./.

***Nơi nhận:***

- Như trên;
- Lãnh đạo Sở;
- Các đơn vị thuộc Sở;
- Lưu: VT.

**KT. GIÁM ĐỐC  
PHÓ GIÁM ĐỐC**

**Đỗ Minh Trí**