UBND TỈNH TÂY NINH
SỞ GIÁO DỤC VÀ ĐÀO TẠO

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

Số: 130 /SGDĐT-QLCL-CĐS

Tây Ninh, ngày 16 tháng 7 năm 2025

Về việc triển khai bảo đảm an toàn thông tin cho các nền tảng số dùng chung

Kính gửi:
- Các phòng thuộc Sở Giáo dục và Đào tạo;
- Hiệu trưởng các trường phổ thông;
- Hiệu trưởng các trường mầm non, mẫu giáo;
- Hiệu trưởng Trường Khuyết tật tỉnh Tây Ninh;
- Giám đốc trung tâm GDTX, trung tâm GDNN-GDTX;
- Giám đốc Trung tâm Giáo dục thường xuyên - Kỹ thuật tổng hợp;
- Giám đốc Trung tâm Nuôi dạy trẻ Khiếm thị tỉnh Tây Ninh;
- Hiệu trưởng Trường Trung cấp Kinh tế - Kỹ thuật Tây Ninh.

Thực hiện Công văn số 56/SKHCN-CĐS ngày 08/7/2025 của Sở Khoa học và Công nghệ về việc triển khai bảo đảm an toàn thông tin cho các nền tảng số dùng chung của tỉnh, Giám đốc Sở Giáo dục và Đào tạo yêu cầu lãnh đạo các đơn vị, trường học thực hiện như sau:

1. Tổ chức tuyên truyền, phổ biến, quán triệt cho công chức, viên chức nắm rõ Luật An ninh mạng năm 2018, Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng, Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân; hướng dẫn các biện pháp tăng cường bảo đảm an ninh mạng cho hệ thống thông tin quan trọng về an ninh quốc gia. Phân công trách nhiệm cụ thể trong chỉ đạo, triển khai thực hiện công tác bảo vệ an ninh mạng, bảo vệ hệ thống thông tin trọng yếu, bảo vệ dữ liệu cá nhân; xử lý nghiêm theo quy định các vụ việc gây mất an ninh mạng, lộ mất bí mật nhà nước, vi phạm dữ liệu cá nhân trên không gian mạng.

2. Tổ chức tuyên truyền, phổ biến nhằm nâng cao nhận thức, trách nhiệm của công chức, viên chức đối với công tác đảm bảo an ninh, an toàn hệ thống mạng, bảo vệ bí mật nhà nước, không tiết lộ thông tin dữ liệu cá nhân trên không gian mạng; thường xuyên cập nhật, thực hiện nghiêm các thông báo, cảnh báo của cơ quan chuyên trách về các loại hình tấn công mạng, tội phạm mạng, tội phạm sử dụng công nghệ cao, nguy cơ mất an ninh mạng, xâm phạm dữ liệu cá nhân.

3. Cài đặt sử dụng phần mềm có bản quyền (*hệ điều hành, phần mềm văn phòng, phần mềm phòng chống mã độc và các phần mềm ứng dụng khác*) và

thường xuyên cập nhật các bản vá bảo mật cho hệ điều hành và các phần mềm ứng dụng để khắc phục các lỗ hổng bảo mật.

4. Quán triệt công chức, viên chức không được tải hoặc cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc hoặc không được phép của cơ quan. Hạn chế tối đa việc kết nối các thiết bị lưu trữ bên ngoài (USB, ổ cứng di động,...), không lưu tài khoản và mật khẩu đăng nhập trên trình duyệt web.

5. Cấu hình vô hiệu hóa/tắt tài khoản "Guest" hoặc các tài khoản khách trên máy tính cá nhân, vô hiệu hóa/tắt các kết nối không dây như Bluetooth, Wifi trên các thiết bị không có nhu cầu sử dụng hoặc không làm việc. Vô hiệu hóa các tính năng điều khiển từ xa (Remote Desktop, TeamViewer, AnyDesk,...) và truyền phát không dây (Chromecast, Miracast,...) trên các thiết bị máy tính làm việc.

6. Chỉ đạo các cán bộ, công chức, viên chức định kỳ 06 tháng/lần thực hiện *thay đổi mật khẩu* các tài khoản được cấp đang sử dụng các hệ thống thông tin dùng chung của tỉnh *(Hệ thống giải quyết thủ tục hành chính, phân hệ Một cửa điện tử, Hệ thống Quản lý văn bản và điều hành, Hệ thống Quản lý cán bộ công chức,...)* theo đúng quy định, yêu cầu về đảm bảo an toàn thông tin, cụ thể: Độ dài mật khẩu *tối thiểu từ 8 ký tự trở lên*, bao gồm sự kết hợp đầy đủ giữa chữ hoa, chữ thường, ký tự số (1,2,3,..) và ký tự đặc biệt (@, #, $, !, %, * , ?, &,…); sử dụng mật khẩu khác nhau cho từng tài khoản để đề phòng việc tin tặc sử dụng một mật khẩu để truy cập vào tất cả các tài khoản. Tuyệt đối không tiết lộ mật khẩu của cá nhân cho người khác, cũng như giao tài khoản mật khẩu cho người khác sử dụng thay mình.

7. Các đơn vị trường học chú trọng các biện pháp bảo mật đối với hệ thống mạng nội bộ cần cấu hình phân vùng mạng rõ ràng: Thực hiện phân vùng mạng rõ ràng thành các vùng riêng biệt như: Vùng nội bộ (dành riêng cho cán bộ công chức, viên chức); Vùng khách (dành cho người dân truy cập Wifi công cộng); Đặt mật khẩu mạnh cho các thiết bị phát Wifi (bao gồm chữ hoa, chữ thường, số, ký tự đặc biệt và có độ dài tối thiểu 8 ký tự), tắt tính năng WPS, thay đổi mật khẩu mặc định và định kỳ thay đổi mật khẩu.

8. Chủ động rà soát định kỳ nội dung trên Trang thông tin điện tử của đơn vị đảm bảo các thông tin được đăng tải (như thủ tục hành chính, chính sách, thông báo, tin tức) luôn chính xác, đầy đủ và cập nhật theo quy định mới nhất, đảm bảo.

9. Tiến hành kiểm tra rà soát, xây dựng hoàn thiện các quy định, quy trình, quy chế, hướng dẫn về bảo vệ an toàn, an ninh mạng.

10. Cử công chức, viên chức tham gia đầy đủ các đợt tập huấn, bồi dưỡng, nâng cao kiến thức, kỹ năng cho đội ngũ phụ trách công nghệ thông tin, an ninh

mạng nhằm đáp ứng năng lực, yêu cầu bảo vệ an ninh mạng và bí mật nhà nước trên không gian mạng.

Giám đốc Sở Giáo dục và Đào tạo yêu cầu thủ trưởng các đơn vị nghiêm túc nội dung công văn này. Trong quá trình triển khai thực hiện nếu đơn vị có khó khăn, vướng mắc liên hệ Ông Trần Ngọc Linh, Phòng Quản lý chất lượng – Chuyển đổi số, số điện thoại: 0975.558.587 (đính kèm Công văn số 56/SKHCN-CĐS ngày 08/7/2025 của Sở Khoa học và Công nghệ)./.

Nơi nhận:
- Như trên;
- GĐ, các P.GĐ Sở;
- Phòng VHXH xã, phường;
- Lưu: VT, QLCL-CĐS.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
TỈNH TÂY NINH

Phan Minh Tùng