

**ỦY BAN NHÂN DÂN
THỊ XÃ HOÀI NHƠN**

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

Số: /UBND-VX

Hoài Nhơn, ngày tháng 4 năm 2023

V/v tăng cường các biện pháp đảm bảo
an toàn thông tin đối với
các hệ thống thông tin

Kính gửi:

- Các cơ quan, đơn vị liên quan;
- UBND các xã, phường.

Thực hiện Công văn số 429/STTTT-BCVT&CNTT ngày 18/4/2023 của Sở Thông tin và Truyền thông về việc tăng cường các biện pháp đảm bảo an toàn thông tin đối với các hệ thống thông tin.

Nhằm tăng cường các biện pháp đảm bảo an toàn thông tin đối với các hệ thống thông tin do các cơ quan, đơn vị, UBND các xã, phường quản lý, vận hành, UBND thị xã yêu cầu các cơ quan, đơn vị, UBND các xã, phường tập trung thực hiện các nội dung sau:

1. Triển khai đảm bảo an toàn thông tin đối với các hệ thống thông tin do cơ quan, đơn vị, UBND các xã, phường quản lý, vận hành. Bố trí kinh phí đầu tư bảo đảm an toàn hệ thống thông tin theo cấp độ (*theo Kế hoạch số 59/KH-UBND ngày 10/4/2023 của UBND thị xã*) và phần mềm diệt virus có bản quyền để bảo vệ an toàn hệ thống mạng của cơ quan, đơn vị, UBND các xã, phường và thông tin dữ liệu cá nhân của người sử dụng. Trong đó, quan tâm mua sắm phần mềm diệt virus bản quyền cho các máy tính thường xuyên sử dụng để ký số, ban hành văn bản điện tử, máy tính tham gia hệ thống đấu thầu qua mạng và kết nối các cơ sở dữ liệu của tỉnh, quốc gia...

2. Tăng cường công tác bảo vệ thông tin cá nhân trên môi trường mạng, định kỳ thay đổi mật khẩu đối với các tài khoản được giao/cấp sử dụng đăng nhập các hệ thống thông tin dùng chung toàn tỉnh (*phần mềm Dịch vụ công, Một cửa, phần mềm Quản lý cán bộ công chức, phần mềm Quản lý tiền lương...*); Đối với các tài khoản được cấp mật khẩu mặc định phải tiến hành đổi mật khẩu khi đăng nhập lần đầu theo hướng dẫn của đơn vị phát triển phần mềm.

3. Rà soát các nội dung, đường dẫn, thư mục được công khai trên các Cổng thông tin điện tử do cơ quan, đơn vị và UBND các xã, phường quản lý để kịp thời gỡ bỏ các đường dẫn có kết nối đến các website có nội dung không phù hợp (*quảng cáo, cá độ, cờ bạc trực tuyến...*) gây ảnh hưởng đến hoạt động, uy tín của các cơ quan nhà nước, tiềm ẩn các nguy cơ mất an toàn thông tin.

4. Thực hiện giám sát bảo vệ đối với hệ thống thông tin do cơ quan, đơn vị và UBND các xã, phường quản lý, vận hành; Định kỳ thực hiện kiểm tra, đánh giá, rà quét các lỗ hổng bảo mật tồn tại trong hệ thống để tìm ra các điểm yếu gây mất an toàn thông tin.

5. Xây dựng phương án ứng cứu, khắc phục sự cố mất an toàn thông tin đối với các hệ thống thông tin tại cơ quan, đơn vị và UBND các xã, phường kịp thời báo cáo UBND thị xã (qua Phòng Văn hóa và Thông tin) khi xảy ra các sự cố mất an toàn thông tin theo quy định.

6. Chỉ đạo cán bộ, công chức, viên chức và người lao động của cơ quan, đơn vị và UBND các xã, phường tích cực tham gia vào các chiến dịch rà quét làm sạch mã độc trên không gian mạng; thực hiện đăng ký tín nhiệm mạng đối với các website do cơ quan, đơn vị địa phương quản lý.

UBND thị xã yêu cầu các cơ quan, đơn vị và UBND các xã, phường triển khai thực hiện để đảm bảo các hệ thống thông tin được vận hành thông suốt, ổn định phục vụ công tác chuyển đổi số toàn diện các lĩnh vực trên địa bàn thị xã./.

Nơi nhận:

- Như trên;
- Lưu: VT.

**KT. CHỦ TỊCH
PHÓ CHỦ TỊCH**

Phạm Văn Chung