

Số: 8722 /UBND-KGVX

Biên Hòa, ngày 31 tháng 5 năm 2024

V/v tăng cường công tác đảm  
bảo an ninh mạng hệ thống  
thông tin trọng yếu trên địa  
bàn thành phố

Kính gửi:  
- Các cơ quan, đơn vị thành phố;  
- UBND 30 phường, xã.

Thực hiện Văn bản số 66/TBATANM-THNC ngày 20/5/2024 của UBND tỉnh Đồng Nai về việc tăng cường công tác đảm bảo an ninh mạng hệ thống thông tin trọng yếu trên địa bàn tỉnh Đồng Nai (Văn bản gửi kèm), Chủ tịch UBND thành phố Biên Hòa yêu cầu Thủ trưởng các cơ quan, đơn vị thành phố, Chủ tịch UBND 30 phường, xã khẩn trương triển khai thực hiện các nội dung sau:

1. Quán triệt, thực hiện nghiêm Luật An ninh mạng năm 2018, Nghị định SỐ 53/2022/ND-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... Cụ thể hóa trách nhiệm của đơn vị, tổ chức, cá nhân trong công tác bảo vệ an ninh mạng hệ thống thông tin trọng yếu, bảo vệ dữ liệu cá nhân; định kỳ, đột xuất kiểm tra, giám sát việc thực hiện các quy định về bảo vệ an ninh mạng, bảo vệ hệ thống thông tin trọng yếu, xử lý nghiêm theo quy định các vụ việc gây mất an ninh mạng, lộ, mất bí mật nhà nước, dữ liệu cá nhân trên không gian mạng.

2. Tổ chức tuyên truyền, phổ biến trong toàn hệ thống chính trị, các cơ quan, đơn vị nhằm nâng cao nhận thức, trách nhiệm đối với công tác đảm bảo an ninh, an toàn hệ thống mạng, bảo vệ bí mật nhà nước, 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, thông tin dữ liệu cá nhân.

3. Khẩn trương, ưu tiên tổ chức kiểm tra an ninh mạng; rà soát, gỡ bỏ mã độc trên máy tính (nếu có); sao lưu dự phòng dữ liệu quan trọng; tăng cường giám sát an ninh mạng để kịp thời phát hiện hoạt động tấn công mạng. Tiến hành rà soát, xây dựng, hoàn thiện các quy định, quy trình, quy chế, hướng dẫn về bảo vệ an ninh mạng, đồng thời rà soát việc tuân thủ của bộ phận kỹ thuật,



cán bộ, công chức, viên chức, người lao động đối với chính sách quản lý, quy chế bảo đảm an ninh mạng, quy trình quản trị, vận hành, ứng cứu sự cố, kiểm soát truy cập tài khoản quản trị đối với các hệ thống thông tin theo tài liệu **“Hướng dẫn các biện pháp bảo đảm an ninh mạng cho hệ thống thông tin quan trọng về an ninh quốc gia”** tại Thông báo số 2009/TB-A0S-TTANMOG ngày 18.02.2024 của các Mô hình mạng và phòng, chống tội phạm sử dụng công nghệ cao - Bộ Công an (sao gửi kèm theo).

Chủ quản các hệ thống thông tin chủ động xây dựng, triển khai phương án, tổ chức diễn tập phòng, chống tấn công mạng và ứng phó, khắc phục sự cố an ninh mạng theo quy định; thiết lập các kênh thông tin trao đổi, chia sẻ thông tin, thông báo sự cố an ninh mạng với các lực lượng chuyên trách bảo vệ an ninh mạng.

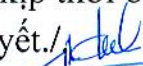
4. Tăng cường đầu tư về công nghệ, hệ thống kỹ thuật đảm bảo các quy chuẩn, tiêu chuẩn theo quy định, tránh tình trạng tập trung chuyển đổi số mà thiếu sự quan tâm tới công tác bảo đảm an toàn, an ninh mạng; ưu tiên sử dụng sản phẩm, thiết bị mạng được kiểm tra, đánh giá đảm bảo an ninh mạng. Chủ quản hệ thống thông tin trọng yếu khẩn trương kết nối với hệ thống giám sát của Trung tâm An ninh mạng quốc gia đặt tại Bộ Công an để kịp thời phát hiện, cảnh báo, giám sát, khắc phục các sự cố, tình huống nguy cấp mất an ninh mạng.

5. Tập trung đầu tư, phân bổ kinh phí, bố trí nhân lực bảo vệ an ninh mạng: thường xuyên tổ chức tập huấn, bồi dưỡng, nâng cao kiến thức, kỹ năng cho cán bộ, đảng viên, đội ngũ chuyên trách công nghệ thông tin, an ninh mạng tại các cơ quan, đơn vị đáp ứng năng lực, yêu cầu bảo vệ an ninh mạng và bí mật nhà nước trên không gian mạng.

6. Các đơn vị có hoạt động thu thập, xử lý dữ liệu cá nhân tiến hành rà soát tổng thể, phân loại dữ liệu cá nhân đã thu thập, đang xử lý; xác định trách nhiệm bảo vệ tương ứng với từng loại dữ liệu cá nhân; thực hiện việc đánh giá tác động và chuyển dữ liệu cá nhân ra nước ngoài... theo đúng quy định tại Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân. Rà soát, đánh giá quy trình thu thập, xử lý dữ liệu cá nhân, đề xuất ban hành các biện pháp quản lý phù hợp với quy mô, mức độ xử lý dữ liệu cá nhân của cơ quan, đơn vị; nghiên cứu chỉ định bộ phận có chức năng bảo vệ dữ liệu cá nhân, nhân sự phụ trách xử lý dữ liệu cá nhân nhạy cảm (nếu có); đối với cơ quan nhà nước, các doanh nghiệp đang xử lý khối lượng lớn dữ liệu cá nhân, đặc biệt là dữ liệu cá nhân nhạy cảm thường xuyên kiểm tra, đánh giá đảm bảo an ninh trong hoạt động xử lý. Xử lý nghiêm các hành vi chuyển giao, mua bán dữ liệu cá nhân trái phép. Trong trường hợp phát hiện xảy ra vi phạm quy định bảo

vệ dữ liệu cá nhân thông báo cho cơ quan chuyên trách bảo vệ dữ liệu cá nhân Công an tỉnh để phối hợp xử lý.

7. Nếu đề xảy ra sai phạm, xem xét trách nhiệm của chủ quản hệ thống thông tin, cán bộ nhân viên chuyên trách và các cá nhân có liên quan theo quy định của pháp luật.

Trong quá trình thực hiện có khó khăn, vướng mắc, kịp thời báo cáo và có ý kiến đề xuất UBND thành phố Biên Hòa xem xét giải quyết. / 

**Nơi nhận:**

- Như trên (thực hiện);
- UBND tỉnh Đồng Nai (b/c);
- Thường trực Thành ủy;
- Thường trực HĐND TP;
- Chủ tịch, các Phó Chủ tịch UBND TP;
- UBMTTQVN TP, các Hội, Đoàn thể TP;
- Ban Tuyên giáo Thành ủy;
- Chánh, các PVP HĐND-UBND TP;
- Lưu: VT, KGVX<sub>TP</sub>.

**CHỦ TỊCH**



**Đỗ Khôi Nguyên**