

ĐỀ CƯƠNG

**Báo cáo kết quả tự kiểm tra công tác bảo đảm an ninh mạng, an toàn
Thông tin và bảo vệ bí mật nhà nước trên không gian mạng năm 2025**
(Ban hành kèm theo Kế hoạch số: /KH-UBND ngày /5/2025 của UBND tỉnh)

I. KẾT QUẢ TỰ KIỂM TRA

1. Việc tổ chức triển khai thực hiện quy định của pháp luật về bảo đảm an ninh mạng, an toàn thông tin và bảo vệ bí mật nhà nước (BMNN) trên không gian mạng

- Công tác tuyên truyền, phổ biến, quán triệt và tổ chức triển khai thực hiện Luật An ninh mạng, Luật Bảo vệ BMNN và các văn bản hướng dẫn thi hành; các văn bản chỉ đạo của các cơ quan, tổ chức Trung ương, của Tỉnh ủy, Ủy ban nhân dân tỉnh và Tiểu ban liên quan đến công tác bảo đảm an ninh mạng, an toàn thông tin và bảo vệ BMNN trên không gian mạng, trọng tâm là: Chỉ thị số 02/CT-TTg ngày 04/7/2018 về công tác bảo vệ BMNN trên không gian mạng¹; Chỉ thị số 14/CT-TTg ngày 25/5/2018 về nâng cao năng lực phòng chống phần mềm độc hại²; Công văn số 157/UBND-NC ngày 13/4/2022 của UBND tỉnh về việc tiếp tục triển khai thực hiện Chỉ thị của Thủ tướng Chính Phủ về công tác bảo vệ BMNN trên không gian mạng và phòng, chống phần mềm độc hại; Công tác triển khai các Kế hoạch của Tiểu ban an toàn, an ninh mạng tỉnh.

Việc ban hành các văn bản hướng dẫn, tổ chức thực hiện chế độ báo cáo các văn bản nêu trên tại cơ quan, đơn vị địa phương.

2. Kiểm tra, đánh giá thực trạng công tác bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin của các cơ quan, đơn vị, địa phương

2.1. Tổng rà soát, thống kê số lượng các trang thiết bị tin học, phương tiện, trang thiết bị phục vụ công tác có liên quan đến hệ thống thông tin của cơ quan, đơn vị đến thời điểm hiện tại (*Hệ thống máy tính, mạng máy tính; các thiết bị kết nối ngoại vi như: USB, ổ cứng rời, điện thoại thông minh, máy tính bảng...; trang/cổng thông tin điện tử; trang mạng xã hội...*).

2.2. Việc triển khai các hoạt động bảo vệ an ninh mạng.

- Việc xây dựng, hoàn thiện quy định, quy chế sử dụng mạng máy tính nội bộ, mạng máy tính có kết nối Internet; phương án bảo đảm an ninh mạng đối với

¹ UBND tỉnh triển khai tại Công văn số 206/UBND-NC, ngày 12/7/2018.

² UBND tỉnh triển khai tại Công văn số 10026/UBND-NC, ngày 15/11/2018.

các hệ thống thông tin; phương án ứng cứu, khắc phục sự cố an ninh mạng.

- Ứng dụng, triển khai phương án, biện pháp, công nghệ bảo đảm an ninh đối với các hệ thống thông tin và nội dung thông tin, tài liệu được lưu trữ, soạn thảo, truyền tải trên hệ thống thông tin thuộc phạm vi quản lý.

- Công tác bảo đảm an ninh mạng trong hoạt động cung cấp, trao đổi, thu thập thông tin với cơ quan, tổ chức, cá nhân; chia sẻ thông tin, tài liệu trong nội bộ với cơ quan, đơn vị khác.

- Công tác thanh tra, tự kiểm tra của cơ quan, đơn vị địa phương: Số cuộc thanh tra, tự kiểm tra? Việc xử lý vi phạm (*nếu có*)? Việc thực hiện những kiến nghị sau thanh tra, tự kiểm tra?

- Việc rà soát khắc phục những sơ hở, điểm yếu, lỗ hổng bảo mật đối với hệ thống thông tin thuộc phạm vi quản lý theo yêu cầu, thông báo, khuyến cáo các cơ quan, đơn vị chuyên trách về an ninh mạng (*nếu có*).

- Kiểm tra việc khắc phục hạn chế, thiếu sót đã chỉ ra trước đây của các Đoàn kiểm tra công tác bảo vệ BMNN đối với đơn vị trong công tác bảo đảm an ninh mạng, an toàn thông tin và bảo vệ BMNN trên không gian mạng.

2.3. Kiểm tra, đánh giá thực trạng an ninh mạng, an toàn thông tin đối với máy tính, hệ thống mạng máy tính, phương tiện điện tử, hệ thống thông tin và các trang/công thông tin điện tử.

- Kiểm tra, rà soát, phát hiện điểm yếu, lỗ hổng bảo mật, mã độc trên các máy chủ, máy tính (*nội bộ, độc lập, Internet*), các thiết bị lưu trữ ngoại vi, trang/công thông tin điện tử, các hệ thống công nghệ thông tin khác và các nguy cơ lộ, mất BMNN trên không gian mạng tại các cơ quan, đơn vị, địa phương.

- Kiểm tra hoạt động quản lý, quản trị vận hành và sử dụng các thiết bị mạng; chính sách an ninh mạng, an toàn thông tin cho các hệ thống công nghệ thông tin, như: Việc nâng cấp, cập nhật lỗ hổng bảo mật hệ điều hành, phần mềm ứng dụng, chính sách mật khẩu; kiểm soát và giới hạn truy cập; cơ chế sao lưu, dự phòng và khắc phục sự cố...

2.4. Việc triển khai tổ chức thực hiện công tác bảo đảm an ninh mạng, an toàn thông tin và bảo vệ BMNN trên không gian mạng tại các cơ quan, đơn vị, địa phương đến thời điểm hiện tại.

- Nhân sự quản lý, vận hành; số lượng trang thiết bị, phần mềm phục vụ công tác lưu trữ, soạn thảo, truyền tải tài liệu liên quan đến BMNN. Việc giao quản lý, sử dụng các trang thiết bị của đơn vị đối với tổ chức, cá nhân thuộc thẩm quyền quản lý.

- Những vấn đề cần chú ý liên quan đến an toàn, an ninh mạng của hệ thống; những vụ việc tấn công mạng, gián điệp mạng; lộ mất BMNN trên không

gian mạng tại cơ quan, đơn vị địa phương đã xảy ra trước đây và kết quả xử lý, khắc phục.

3. Công tác quản lý thông tin, tài liệu, dữ liệu lưu trữ trong hệ thống thông tin của các cơ quan, đơn vị địa phương.

II. NHẬN XÉT, ĐÁNH GIÁ

1. Ưu điểm.

2. Hạn chế, thiếu sót, nguyên nhân của hạn chế, thiếu sót.

3. Những khó khăn, vướng mắc trong quá trình triển khai thực hiện công tác bảo đảm an ninh mạng, an toàn thông tin và bảo vệ BMNN trên không gian mạng tại cơ quan, đơn vị, địa phương.

III. KIẾN NGHỊ, ĐỀ XUẤT

Nêu cụ thể những kiến nghị, đề xuất trong việc thực hiện công tác bảo đảm an ninh mạng, an toàn thông tin và bảo vệ BMNN trên không gian mạng tại cơ quan, đơn vị, địa phương.