BẢO HIỂM XÃ HỘI VIỆT NAM	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 182 /BHXH-CNTT V/v tăng cường công tác bảo đảm an toàn thông tin mạng trong dịp Tết Nguyên đán Giáp Thìn	*Hà Nội, ngày* 22 *tháng* 01 *năm 2024*

Kính gửi:
- Văn phòng Bảo hiểm xã hội Việt Nam,
- Các đơn vị sự nghiệp trực thuộc Bảo hiểm xã hội Việt Nam,
- Bảo hiểm xã hội các tỉnh, thành phố trực thuộc Trung ương.

(*Sau đây gọi chung là các đơn vị*)

Sự cố mất an toàn thông tin mạng nghiêm trọng thường được ghi nhận tại thời điểm diễn ra dịp nghỉ lễ của đất nước, các đối tượng thường tăng cường tấn công mạng vào các hệ thống thông tin quan trọng hoặc lợi dụng không gian mạng để phát tán thông tin xấu độc, lừa đảo trong các dịp này. Nhằm nâng cao cảnh giác và trách nhiệm bảo đảm an toàn thông tin mạng theo quy định của pháp luật trong thời gian diễn ra dịp nghỉ lễ Tết Nguyên đán Giáp Thìn, Bảo hiểm xã hội (BHXH) Việt Nam yêu cầu các đơn vị triển khai một số biện pháp như sau:

1. Rà soát máy chủ, máy trạm trong hệ thống mạng, bảo đảm các máy chủ, máy trạm được triển khai đầy đủ các giải pháp kỹ thuật bảo đảm an toàn thông tin, bảo vệ bí mật nhà nước trên không gian mạng của ngành BHXH Việt Nam; Kiểm tra và bóc gỡ các phần mềm độc hại cho toàn bộ máy chủ, máy trạm trong hệ thống mạng, trong đó cần ưu tiên xử lý các máy chủ, máy trạm có tài khoản, địa chỉ IP … nằm trong danh sách cảnh báo của BHXH Việt Nam (Trung tâm Công nghệ thông tin) trong Báo cáo kỹ thuật tình hình an toàn thông tin hàng tháng.

2. Phân công lực lượng bảo đảm an toàn thông tin của đơn vị triển khai trực giám sát, tăng cường theo dõi thường xuyên, liên tục các hệ thống giám sát an toàn thông tin tập trung, hệ thống phòng chống mã độc tập trung, kênh cảnh báo của BHXH Việt Nam (Trung tâm Công nghệ thông tin), các cơ quan có chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công, bảo đảm sẵn sàng ứng cứu khi phát hiện có dấu hiệu bị khai thác, tấn công mạng và khắc phục sự cố an toàn thông tin mạng.

3. Chủ động rà soát các lỗ hổng, điểm yếu trên các máy chủ, máy trạm và các thiết bị thuộc phạm vi quản lý; Triển khai các giải pháp phòng ngừa và khắc phục triệt để các lỗ hổng, điểm yếu đã được BHXH Việt Nam (Trung tâm Công nghệ thông tin) cảnh báo, đặc biệt là các lỗ hổng bảo mật ảnh hưởng mức cao và nghiêm trọng trong các sản phẩm Microsoft gửi trong năm 2023.

4. Tổ chức tuyên truyền, nâng cao nhận thức cơ bản kỹ năng về an toàn thông tin mạng, cảnh giác về thông tin xấu độc, tin giả và thông tin lừa đảo trên không gian mạng cho công chức, viên chức và người lao động trong đơn vị.

5. Trung tâm Công nghệ thông tin tổ chức lực lượng bảo đảm an toàn thông tin trực giám sát 24/7; Thực hiện công tác điều phối và xử lý sự cố tấn công mạng trên Nền tảng Điều phối xử lý sự cố an toàn thông tin mạng quốc gia (IRLab); Bảo đảm duy trì kết nối liên tục tới hệ thống kỹ thuật của Trung tâm Giám sát an toàn không gian mạng quốc gia để được hỗ trợ giám sát, phát hiện và cảnh bảo sớm, xử lý.

Đầu mối liên hệ, hỗ trợ của BHXH Việt Nam (Trung tâm Công nghệ thông tin): Phòng Quản lý Hạ tầng và An toàn thông tin, Ông Nguyễn Tuấn Minh, số điện thoại 0964937180, thư điện tử: minhnt1@vss.gov.vn. Trung tâm Điều hành hệ thống thông tin ngành BHXH, số điện thoại: 0984391786, thư điện tử: noc@vss.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Tổng Giám đốc (để b/c);
- Các Phó Tổng Giám đốc;
- Các đơn vị trực thuộc BHXHVN;
- VPĐU, VPBCSĐ, VPHĐQL;
- Lưu: VT, CNTT.

KT. TỔNG GIÁM ĐỐC
PHÓ TỔNG GIÁM ĐỐC

BẢO HIỂM XÃ HỘI VIỆT NAM

Chu Mạnh Sinh