ĐẢNG BỘ TỈNH LÂM ĐỒNG
HUYỆN ỦY LẠC DƯƠNG
*
Số 264-CV/HU
V/v đảm bảo an ninh, an toàn thông tin mạng và bảo vệ bí mật nhà nước

ĐẢNG CỘNG SẢN VIỆT NAM
Lạc Dương, ngày 16 tháng 7 năm 2021

Kính gửi: - Ủy ban nhân dân huyện,
- Các cơ quan, đơn vị, mặt trận, đoàn thể huyện,
- Các tổ chức cơ sở đảng trực thuộc.

Thời gian qua, việc ứng dụng công nghệ thông tin trong hoạt động của các cấp ủy đảng, chính quyền, cơ quan, đơn vị trên địa bàn huyện được đẩy mạnh, bảo đảm khai thác hiệu quả tài nguyên mạng máy tính; các phần mềm chuyên ngành của Đảng, Nhà nước được ứng dụng rộng rãi tại các cơ quan, đơn vị đã mang lại hiệu quả thiết thực trong trao đổi thông tin và xử lý công việc, dần thay đổi nhận thức, phong cách, lề lối làm việc của cán bộ, đảng viên, công chức, viên chức, phục vụ tốt hơn cho công tác chuyên môn, nâng cao hiệu quả công tác lãnh đạo, chỉ đạo, điều hành của cấp ủy đảng, chính quyền các cấp, góp phần phát triển kinh tế - xã hội, đảm bảo quốc phòng - an ninh, xây dựng Đảng và hệ thống chính trị tại địa phương.

Tuy nhiên, qua nắm bắt tình hình, công tác đảm bảo an ninh, an toàn thông tin mạng, bảo vệ bí mật nhà nước tại một số cơ quan, đơn vị vẫn chưa được quan tâm đúng mức, chưa nhận thức đầy đủ tầm quan trọng của công tác đảm bảo an toàn thông tin mạng, bảo vệ bí mật nhà nước; thậm chí có một số cơ quan, đơn vị, cá nhân còn chủ quan, lơ là, sơ hở trong quản lý thông tin nội bộ và thông tin bí mật nhà nước dẫn đến nguy cơ mất an toàn thông tin.

Để khắc phục những tồn tại, hạn chế nêu trên, nhằm đảm bảo an ninh, an toàn thông tin mạng, bảo vệ bí mật nhà nước trên địa bàn huyện Lạc Dương; ***Thường trực Huyện ủy yêu cầu các cấp ủy đảng, thủ trưởng các cơ quan, ban, ngành, đoàn thể huyện thực hiện tốt những nội dung sau:***

1. Thường xuyên tuyên truyền, phổ biến nâng cao nhận thức cho cán bộ, đảng viên, công chức, viên chức tại cơ quan, đơn vị, địa phương về tầm quan trọng của công tác đảm bảo an ninh, an toàn thông tin mạng, bảo vệ bí mật nhà nước trong tình hình hiện nay; từ đó, quán triệt thực hiện nghiêm túc các chủ trương, đường lối, quy định của Đảng, chính sách, pháp luật của Nhà nước liên quan đến an ninh, an toàn thông tin, bảo vệ bí mật Nhà nước, trọng tâm là: Luật An toàn thông tin mạng, Luật An ninh mạng, Luật Bảo vệ bí mật nhà nước và các văn bản chỉ đạo, hướng dẫn thi hành [1].

---

[1] Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ; Thông tư 03/2017/TT-BTTTT ngày 24/4/2017, Thông tư 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ trưởng Bộ Thông tin và truyền thông; Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ; Nghị định 26/2020/NĐ-CP ngày 28/02/2020 của Chính phủ; các Chỉ thị 02/CT-TTg ngày 04/7/2018, 14/CT-TTg ngày 25/5/2018, 02/CT-TTg ngày 15/11/2019 của Thủ tướng Chính phủ…

2. Thực hiện nghiêm Luật số 29/2018/QH14 ngày 15/11/2018 của Quốc hội về bảo vệ bí mật nhà nước, Nghị định số 26/2020/NĐ-CP ngày 28/02/2020 của Chính phủ quy định chi tiết thi hành một số điều của Luật Bảo vệ bí mật nhà nước, Thông tư số 24/2020/TT-BCA ngày 10/3/2020 của Bộ trưởng Bộ Công an về ban hành biểu mẫu sử dụng trong công tác bảo vệ bí mật nhà nước. Trước mắt cần tập trung tự kiểm tra, rà soát về việc xác định bí mật nhà nước và độ mật của bí mật nhà nước; lưu giữ, sao, chụp tài liệu, vật chứa bí mật nhà nước; sử dụng các biểu mẫu trong công tác bảo vệ bí mật nhà nước… tại cơ quan, đơn vị, địa phương quản lý; kịp thời phát hiện những tồn tại, thiếu sót để sớm có biện pháp khắc phục, đảm bảo công tác bảo vệ bí mật nhà nước được thực hiện đúng thẩm quyền, trình tự, thủ tục theo quy định của pháp luật.

3. Nghiêm cấm soạn thảo, lưu trữ, sao chụp thông tin bí mật nhà nước trên máy tính hoặc thiết bị điện tử có tính năng lưu trữ thông tin có kết nối mạng Internet. Không kết nối mạng nội bộ chứa thông tin bí mật nhà nước với mạng Internet và ngược lại. Tăng cường quản lý việc sử dụng thiết bị lưu trữ ngoài (USB, thẻ nhớ, ổ cứng di động…), tuyệt đối không kết nối các thiết bị lưu trữ ngoài để sao chép dữ liệu giữa máy tính soạn thảo nội dung bí mật nhà nước với máy tính hoặc thiết bị, phương tiện điện tử có kết nối Iternet.

Nghiêm cấm chuyển đổi mục đích sử dụng máy tính dùng để soạn thảo, lưu trữ thông tin có nội dung bí mật nhà nước sang máy tính có kết nối Internet và ngược lại mà chưa có giải pháp hủy dữ liệu triệt để. Các thiết bị có lưu trữ nội dung bí mật nhà nước không còn sử dụng phải được xử lý hoặc tiêu hủy theo đúng quy trình, quy định của pháp luật về bảo vệ bí mật nhà nước.

4. Tăng cường trao đổi văn bản, tài liệu công việc qua các phần mềm IDOC, VNPT-Ioffice, hệ thống thư công vụ của tỉnh và các phần mềm chuyên ngành; không trao đổi thông tin bí mật nhà nước qua điện thoại, fax, hộp thư điện tử cá nhân và các dịch vụ gia tăng trên nền Internet (OTT); việc trao đổi thông tin bí mật nhà nước trên mạng phải thực hiện theo Khoản 1, Điều 9 Luật Cơ yếu số 05/2011/QH13 ngày 26/11/2011 của Quốc hội quy định *"Thông tin bí mật nhà nước được truyền bằng các phương tiện thông tin, viễn thông phải được mã hóa bằng mật mã của cơ yếu"*.

5. Tiến hành kiểm tra an ninh thiết bị, phần mềm hệ thống, phần mềm ứng dụng trước khi đưa vào sử dụng và sau khi được nâng cấp, sửa đổi. Định kỳ kiểm tra, rà soát, kích hoạt và thiết lập chức năng tường lửa, chế độ tự động cập nhật bản vá lỗ hổng bảo mật các phiên bản của hệ điều hành Windows trên các máy tính cá nhân tại cơ quan, đơn vị nhằm hạn chế thấp nhất các nguy cơ xâm nhập trái phép. Quán triệt cán bộ, công chức, viên chức của đơn vị không cài đặt phần mềm không rõ nguồn gốc, xuất xứ; không truy cập những Website có nội dung không lành mạnh, không mở những thư điện tử không rõ địa chỉ người gửi… để tránh tối đa việc các phần mềm virus, mã độc sẽ tự động cài đặt vào máy tính cá nhân.

6. Quan tâm đầu tư cơ sở vật chất, trang thiết bị kỹ thuật bảo đảm an ninh mạng, an toàn thông tin, bảo vệ bí mật nhà nước; tăng cường ứng dụng khoa học kỹ thuật và công nghệ mới để kiểm soát thông tin, phòng chống lộ lọt, mất bí mật nhà nước trên không gian mạng. Để đảm bảo an toàn khi sử dụng máy tính cho soạn thảo văn bản có nội dung thuộc bí mật nhà nước, các đơn vị cần bố trí 01 máy tính dùng riêng có đặt mật khẩu truy cập và không kết với mạng nội bộ (LAN), mạng Internet.

7. Khi xảy ra hoặc nghi ngờ xảy ra tình trạng mất an ninh, an toàn thông tin, các cơ quan, đơn vị nhanh chóng khắc phục sự cố, hạn chế thấp nhất mức thiệt hại xảy ra; đồng thời chủ động thông báo cho cơ quan Công an và các ngành chức năng liên quan để phối hợp kiểm tra, đảm bảo an ninh, an toàn thông tin.

Yêu cầu Bí thư các tổ chức cơ sở đảng trực thuộc, Thủ trưởng các cơ quan, ban, ngành, đoàn thể huyện tổ chức quán triệt và triển khai thực hiện nghiêm túc Công văn này; chịu trách nhiệm trước Thường trực Huyện ủy, Chủ tịch Ủy ban nhân dân huyện nếu để xảy ra sự cố mất an ninh, an toàn thông tin mạng, lộ lọt bí mật nhà nước tại cơ quan, đơn vị, địa phương mình quản lý./.

Nơi nhận:
- Như trên,
- Thường trực Huyện ủy,
- Lưu Văn phòng Huyện ủy.

T/M BAN THƯỜNG VỤ
BÍ THƯ

ĐẢNG CỘNG SẢN VIỆT NAM
HUYỆN ỦY LẠC DƯƠNG
ĐẢNG BỘ TỈNH LÂM ĐỒNG

Phạm Triều