ỦY BAN NHÂN DÂN XÃ PHÚC LỘC	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1480/QĐ-UBND	*Phúc Lộc, ngày 12 tháng 6 năm 2026*

QUYẾT ĐỊNH
Ban hành Quy chế bảo đảm an toàn thông tin Hệ thống mạng nội bộ tại UBND xã Phúc Lộc

CHỦ TỊCH ỦY BAN NHÂN DÂN XÃ PHÚC LỘC

Căn cứ Luật Tổ chức chính quyền địa phương ngày 16/6/2025; Căn cứ Luật Công nghệ thông tin ngày 29/6/2006;

Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015; Căn cứ Luật An ninh mạng ngày 12/6/2018;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước; Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; Nghị định số 142/2016/NĐ-CP ngày 14/10/2016 của Chính phủ về ngăn chặn xung đột thông tin trên mạng; Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Quyết định số 2223/QĐ-UBND ngày 14/4/2023 của Ủy ban nhân dân thành phố Hà Nội về việc ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động của cơ quan nhà nước thành phố Hà Nội;

Xét đề nghị của Chánh Văn phòng HĐND & UBND xã.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy chế bảo đảm an toàn thông tin Hệ thống mạng nội bộ tại UBND xã Phúc Lộc"

Quy chế này áp dụng đối với việc quản lý, vận hành toàn bộ hệ thống thông tin của UBND xã, bao gồm: hệ thống mạng nội bộ, hệ thống camera giám sát, trang thông tin điện tử của xã, các hệ thống quản lý điều hành cùng các thành phần công nghệ thông tin khác liên quan.

Điều 2. Quyết định có hiệu lực kể từ ngày ký.

Điều 3. Chánh Văn phòng HĐND & UBND xã, Trưởng phòng Văn hoá - Xã hội; Thủ trưởng các cơ quan, đơn vị có liên quan và các ông (bà) cán bộ, công chức, viên chức, người lao động thuộc UBND xã chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- UBND thành phố Hà Nội;
- Sở KH&CN Hà Nội;
- TT. Đảng uỷ, TT. HĐND xã;
- CT, các PCT UBND xã;
- Các phòng, ban, ngành xã;
- Các thôn trên địa bàn;
- Lưu: VT.

CHỦ TỊCH

U.B.N.D XÃ PHÚC LỘC T.P HÀ NỘI

Lê Văn Thu

ỦY BAN NHÂN DÂN XÃ PHÚC LỘC	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ
Bảo đảm an toàn thông tin Hệ thống mạng nội bộ tại UBND xã Phúc Lộc

(Ban hành kèm theo Quyết định số 1480/QĐ-UBND ngày 12 / 6 /2026 của UBND xã Phúc Lộc)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định các chính sách, biện pháp quản lý và kỹ thuật nhằm bảo đảm an ninh mạng, an toàn thông tin (sau đây viết tắt là ATTT) trong việc xây dựng, vận hành và khai thác các hệ thống thông tin của UBND xã. Hệ thống thông tin của UBND xã bao gồm các thành phần chính: mạng nội bộ (LAN), phần mềm quản lý văn bản điều hành, hệ thống camera giám sát, cổng dịch vụ công trực tuyến của xã, trang thông tin điện tử (cổng thông tin) của xã, cùng các cơ sở hạ tầng, thiết bị, phần mềm và dữ liệu có liên quan.

Điều 2. Đối tượng áp dụng

- Tất cả các phòng, ban, bộ phận chuyên môn và cán bộ, công chức, người lao động thuộc UBND xã Phúc Lộc có sử dụng hoặc quản lý các hệ thống thông tin của UBND xã.

- Cơ quan, tổ chức, cá nhân có kết nối, sử dụng các hệ thống thông tin của UBND xã (ví dụ: người dân, doanh nghiệp sử dụng cổng dịch vụ công trực tuyến).

- Các tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin hoặc dịch vụ đảm bảo an toàn thông tin mạng cho UBND xã Phúc Lộc (nhà thầu bảo trì hệ thống, đơn vị cung cấp thiết bị, v.v.), trong phạm vi các hệ thống thông tin của UBND xã Phúc Lộc

Điều 3. Mục tiêu và nguyên tắc bảo đảm an ninh, an toàn thông tin

1. Bảo vệ thông tin và các hệ thống thông tin của UBND xã tránh khỏi các nguy cơ truy cập trái phép, sử dụng sai mục đích, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại, nhằm đảm bảo tính bảo mật, tính toàn vẹn và tính khả dụng của thông tin và hệ thống.

2. Mọi đơn vị, cá nhân thuộc phạm vi áp dụng Quy chế này có trách nhiệm thực hiện đầy đủ các biện pháp bảo đảm an ninh mạng, an toàn thông tin trong phạm vi nhiệm vụ công việc của mình, tuân thủ các quy định của pháp luật hiện hành và các hướng dẫn của cơ quan có thẩm quyền. Trách nhiệm bảo đảm ATTT gắn liền với trách nhiệm của người đứng đầu đơn vị và từng cá nhân liên quan.

3. Việc bảo đảm an toàn thông tin phải được tiến hành xuyên suốt, đồng bộ trong toàn bộ vòng đời của hệ thống thông tin, từ khâu đầu tư, thiết kế, mua sắm, phát triển, triển khai đến vận hành, nâng cấp, bảo trì và khi ngừng sử dụng hạ tầng, thiết bị, phần mềm, dữ liệu.

4. Các biện pháp bảo đảm ATTT phải được thực hiện một cách tổng thể và hiệu quả, tận dụng tối ưu nguồn lực. Việc đầu tư cho an ninh, an toàn thông tin cần được phối hợp tập trung, tránh trùng lặp, lãng phí. Khuyến khích chia sẻ, dùng chung các giải pháp, tài nguyên bảo mật giữa các hệ thống để nâng cao hiệu quả và tính đồng bộ.

5. Trường hợp có quy định khác về an toàn, an ninh thông tin tại văn bản quy phạm pháp luật hoặc quyết định của cấp có thẩm quyền cao hơn, thì áp dụng quy định của văn bản đó (ví dụ: quy định của cơ quan bộ, ngành Trung ương quản lý ngành dọc, nếu có).

6. Thông tin thuộc Danh mục bí mật nhà nước phải được quản lý, bảo vệ theo đúng quy định của pháp luật về bảo vệ bí mật nhà nước. Đối với thông tin, tài liệu mật, việc soạn thảo, lưu trữ, truyền đưa phải tuân thủ Luật Bảo vệ bí mật nhà nước và các quy định liên quan.

Điều 4. Các hành vi bị nghiêm cấm

1. Nghiêm cấm mọi hành vi xâm phạm an ninh, an toàn thông tin mạng theo quy định tại Điều 7 Luật An toàn thông tin mạng 2015 và Điều 8 Luật An ninh mạng 2018. (Các hành vi này bao gồm, ví dụ: ngăn chặn, can thiệp trái phép vào thông tin trên mạng; tấn công, truy cập trái phép, phá hoại hệ thống thông tin; phát tán thư rác, mã độc; đánh cắp, mua bán trái phép thông tin cá nhân; v.v.).

2. Nghiêm cấm việc tự ý đấu nối hoặc thiết lập các thiết bị mạng trái phép vào mạng nội bộ của UBND xã, bao gồm việc tự ý kết nối các thiết bị phát sóng không dây (Wi-Fi cá nhân, thiết bị cấp phát địa chỉ mạng, v.v.) vào mạng nội bộ, hoặc cùng một máy tính vừa kết nối vào mạng nội bộ của cơ quan vừa kết nối Internet qua thiết bị cá nhân (như modem 3G/4G, điện thoại di động dùng làm hotspot).

3. Nghiêm cấm tự ý vô hiệu hóa, tháo gỡ hoặc thay đổi các biện pháp bảo đảm an toàn thông tin được cài đặt trên thiết bị CNTT của cơ quan; không tự ý thay thế, lắp mới hoặc tráo đổi linh kiện, thiết bị trong hệ thống CNTT của UBND xã khi chưa được phép của bộ phận có thẩm quyền.

4. Các hành vi bị cấm khác liên quan đến an ninh mạng, an toàn thông tin theo quy định của pháp luật (nếu có) đều phải được chấp hành nghiêm túc.

Chương II
CÁC BIỆN PHÁP BẢO ĐẢM AN NINH MẠNG, AN TOÀN THÔNG TIN

Điều 5. Bảo đảm an toàn thông tin trong đầu tư, xây dựng hệ thống

1. Xác định cấp độ hệ thống thông tin: UBND xã (với vai trò đơn vị triển khai hệ thống thông tin) có trách nhiệm tổ chức phân loại và xác định cấp độ an toàn cho mỗi hệ thống thông tin thuộc phạm vi quản lý, ngay từ giai đoạn đầu tư, thiết lập hệ thống. Việc xác định cấp độ an toàn hệ thống thông tin thực hiện theo quy định tại Nghị định 85/2016/NĐ- CP và hướng dẫn tại Thông tư 12/2022/TT-BTTTT. Căn cứ vào cấp độ đã được phê duyệt, UBND xã xây dựng và triển khai phương án bảo vệ hệ thống thông tin tương ứng, đáp ứng các yêu cầu tối thiểu về an toàn theo cấp độ. Hồ sơ đề xuất cấp độ của các hệ thống thông tin phải được lập, thẩm định và trình cấp có thẩm quyền phê duyệt theo quy định.

2. Yêu cầu bảo đảm ATTT khi xây dựng mới hoặc nâng cấp: Khi đầu tư, phát triển, mở rộng hệ thống thông tin của xã (bao gồm phần cứng, phần mềm, mạng), phải tích hợp các yêu cầu an toàn thông tin ngay từ khâu thiết kế, xây dựng.

3. Lựa chọn các thiết bị, giải pháp công nghệ thông tin có tiêu chuẩn bảo mật phù hợp, ưu tiên sản phẩm đã được chứng nhận hợp quy hoặc có uy tín về an toàn thông tin.

4. Phần mềm ứng dụng triển khai tại UBND xã phải được phát triển tuân thủ các quy trình lập trình an toàn, kiểm tra lỗ hổng bảo mật trước khi đưa vào sử dụng. Trường hợp thuê đơn vị ngoài phát triển phần mềm, hợp đồng phải có điều khoản ràng buộc về trách nhiệm bảo đảm ATTT, yêu cầu bàn giao mã nguồn hoặc biện pháp kỹ thuật để kiểm soát chất lượng phần mềm.

- Sau khi kết thúc công việc: Yêu cầu bên thứ ba bàn giao lại tài sản sử dụng của đơn vị trong quá trình triển khai công việc; thu hồi quyền truy cập hệ thống CNTT đã được cấp của bên thứ ba ngay sau khi kết thúc công việc; thay đổi các khóa, mật khẩu nhận bàn giao từ bên thứ ba.

5. Trước khi nghiệm thu, đưa hệ thống thông tin mới vào hoạt động, phải kiểm tra, đánh giá an toàn thông tin. Đối với các hệ thống quan trọng, nên phối hợp đơn vị chuyên môn để đánh giá, thử nghiệm thâm nhập nhằm phát hiện sớm điểm yếu và khắc phục.

- Kế hoạch thử nghiệm và nghiệm thu phải được lập rõ ràng trước khi triển khai, nêu cụ thể phạm vi, phương pháp, thời gian, nguồn lực, tiêu chí nghiệm thu và trách nhiệm các bên.

- Quy trình thử nghiệm và nghiệm thu hệ thống được thực hiện theo trình tự sau: xây dựng kế hoạch thử nghiệm, tổ chức thực hiện thử nghiệm chức năng, kiểm tra an toàn thông tin và thử nghiệm thâm nhập; tổng hợp, đánh giá kết quả thử nghiệm; thực hiện khắc phục các tồn tại, hạn chế phát hiện trong quá trình thử nghiệm; tổ chức nghiệm thu chính thức trước khi đưa hệ thống vào vận hành. Đối với các hệ thống

thông tin quan trọng, việc thử nghiệm, đánh giá và nghiệm thu được thực hiện có sự phối hợp của Công an Thành phố theo quy định. Hồ sơ nghiệm thu, kết quả đánh giá và các tài liệu liên quan phải được phê duyệt, lưu trữ đầy đủ trước khi hệ thống được đưa vào khai thác, sử dụng chính thức.

- Trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống thuộc về Chủ tịch UBND xã (người đứng đầu đơn vị) và bộ phận chuyên trách an toàn thông tin của xã. Đối với các hệ thống quan trọng, phải phối hợp Công an Thành phố thực hiện chức năng quản lý nhà nước về an toàn thông tin mạng trên địa bàn Thành phố để đánh giá, thử nghiệm thâm nhập nhằm phát hiện sớm điểm yếu và khắc phục.

6. Phương án ứng cứu sự cố và bảo đảm liên tục hoạt động: Khi thiết kế hệ thống, cần xây dựng phương án dự phòng và kế hoạch ứng cứu sự cố khẩn cấp.

Đảm bảo hệ thống có khả năng sao lưu, phục hồi dữ liệu và chuyển sang hệ thống dự phòng (nếu có) để duy trì hoạt động liên tục khi xảy ra sự cố nghiêm trọng. Các phương án ứng cứu khẩn cấp tuân thủ quy định tại Quyết định 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ về hệ thống phương án ứng cứu khẩn cấp bảo đảm ATTT mạng quốc gia và các hướng dẫn liên quan.

Điều 6. Bảo đảm an toàn cho hạ tầng kỹ thuật và thiết bị CNTT

1. Hạ tầng kỹ thuật phục vụ hệ thống thông tin (phòng máy chủ, tủ thiết bị mạng, hệ thống điện, điều hòa, cáp mạng, v.v.) phải được bảo vệ tránh các rủi ro vật lý như cháy nổ, nhiệt độ/độ ẩm quá mức, bụi bẩn, sét đánh, mất điện hay sự xâm nhập trái phép của con người.

2. Khu vực đặt máy chủ, thiết bị mạng: Phải bố trí tại phòng hoặc tủ kỹ thuật có khóa an toàn. Việc ra vào khu vực này chỉ dành cho người có nhiệm vụ, và cần ghi vào sổ hoặc hệ thống nhật ký. Nếu điều kiện cho phép, trang bị các biện pháp kiểm soát ra vào và giám sát (camera an ninh) để phát hiện truy cập trái phép.

3. Trang bị đầy đủ thiết bị phòng chống cháy nổ (bình chữa cháy…), thiết bị chống sét, hệ thống lưu điện (UPS) đảm bảo duy trì hoạt động tối thiểu 15 phút khi mất điện lưới. Có phương án chống ngập nước, rò rỉ đối với phòng thiết bị

4. Hệ thống cáp mạng và cổng kết nối: Các đường cáp mạng (LAN, cáp quang WAN) phải đi trong ống bảo vệ kín, tránh bị can thiệp vật lý từ bên ngoài. Các cổng mạng không sử dụng cần được tắt hoặc khóa lại, đặc biệt tại các khu vực công cộng trong trụ sở (phòng họp, sảnh tiếp dân…)

5. Quản lý thiết bị CNTT và phương tiện lưu trữ:

a) UBND xã phải thống kê, kiểm kê tất cả thiết bị CNTT, phần mềm, dữ liệu ít nhất mỗi năm một lần, cập nhật vào sổ hoặc phần mềm quản lý tài sản CNTT. Mỗi thiết bị cần gắn mã tài sản và gán trách nhiệm quản lý cho một cá nhân/bộ phận cụ thể. Cán bộ được giao sử dụng thiết bị có trách nhiệm bảo quản và sử dụng đúng mục đích, tuân thủ quy định an toàn

b) Trước khi đưa thiết bị CNTT mới vào sử dụng, phải kiểm tra, đánh giá mức độ an toàn thông tin. Đối với thiết bị quan trọng (máy chủ, thiết bị mạng chính, thiết bị lưu trữ quan trọng, hoặc thiết bị sử dụng cho công việc liên quan đến bí mật nhà nước), nếu cần thiết, đề nghị cơ quan chuyên môn (ví dụ Công an thành phố) kiểm tra đánh giá an ninh trước khi sử dụng

c) Định kỳ hằng năm, lập kế hoạch kiểm tra, bảo trì, bảo dưỡng tất cả trang thiết bị CNTT của UBND xã. Kịp thời thay thế các linh kiện, thiết bị có dấu hiệu hỏng hóc, xuống cấp để phòng ngừa sự cố.

d) Cá nhân sử dụng thiết bị lưu trữ di động (USB, ổ cứng di động, thẻ nhớ…) để lưu thông tin dữ liệu của cơ quan phải bảo vệ thiết bị và dữ liệu trên đó, tránh làm mất, lộ lọt thông tin. Trường hợp thiết bị chứa dữ liệu của cơ quan bị mất hoặc thất lạc, phải báo cáo ngay lãnh đạo để có biện pháp xử lý.

đ) Khi đem thiết bị có lưu trữ dữ liệu đi bảo hành, sửa chữa bên ngoài hoặc khi thanh lý, ngừng sử dụng, phải thực hiện xóa an toàn dữ liệu. Cụ thể, phải tháo hoặc xóa sạch dữ liệu trên ổ cứng, bộ nhớ trước khi giao thiết bị ra khỏi cơ quan (trừ trường hợp cần giữ lại để khôi phục dữ liệu). Khi thanh lý, cần xóa dữ liệu bằng phần mềm hoặc thiết bị chuyên dụng, hoặc phá hủy vật lý thiết bị lưu trữ nếu chứa thông tin nhạy cảm.

e) Đối với các thiết bị hạ tầng kỹ thuật quan trọng (như máy chủ dịch vụ, thiết bị tường lửa, router chính, thiết bị lưu trữ mạng), cần có phương án dự phòng. Định kỳ kiểm tra, bảo dưỡng để đảm bảo các thông số kỹ thuật của thiết bị luôn ở trạng thái tốt; có kế hoạch thay thế hoặc sửa chữa kịp thời để đảm bảo hệ thống hoạt động liên tục.

Điều 7. Bảo đảm an toàn cho mạng nội bộ và kết nối mạng

1. Mạng nội bộ của UBND xã cần được cấu hình theo mô hình phân lớp, phân vùng hợp lý để hạn chế sự lan truyền sự cố. Tránh tổ chức mạng theo kiểu "phẳng" (mọi máy tính trong cùng một mạng) mà không có phân tách. Nếu UBND xã có nhiều khu vực làm việc tách biệt hoặc có mạng Wi-Fi nội bộ, cần thiết lập các vùng mạng riêng cho từng khu vực, phòng ban quan trọng để cô lập truy cập (ví dụ: tách mạng cho hệ thống camera, mạng cho hệ thống dịch vụ công, mạng cho máy văn phòng thông thường)

2. Cấu hình để Wi-Fi chỉ cho phép truy cập Internet, không được truy cập thẳng vào mạng LAN nội bộ của cơ quan. Đặt tên, mật khẩu Wi-Fi đủ mạnh và bật mã hóa (WPA2 hoặc cao hơn); định kỳ thay đổi mật khẩu Wi-Fi (khuyến nghị ít nhất mỗi quý) . Thông tin về điểm truy cập không dây (tên/SSID, mật khẩu) chỉ cung cấp cho người có nhiệm vụ, không công bố công khai; phải thay đổi mật khẩu ngay khi nghi ngờ bị lộ.

3. Cần triển khai các thiết bị/giải pháp bảo mật mạng thích hợp như tường lửa (firewall), hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS) trên cổng kết nối Internet của UBND xã (hoặc tại trung tâm dữ liệu nếu mạng xã được kết nối qua mạng diện rộng của thành phố). Cấu hình tường lửa để chỉ mở các cổng dịch vụ thực sự cần thiết, chặn các lưu lượng không liên quan. Thường xuyên kiểm tra nhật ký (log) truy cập trên firewall để phát hiện kịp thời các kết nối bất thường.

4. Các hệ thống thông tin (máy chủ, máy trạm, thiết bị mạng) của UBND xã phải được cấu hình ghi nhật ký đầy đủ các sự kiện quan trọng (như đăng nhập, đăng xuất, thay đổi cấu hình, truy cập dữ liệu) và lưu trữ các nhật ký này trong thời gian tối thiểu theo quy định (ví dụ 3-6 tháng hoặc hơn, tùy hệ thống). Bộ phận phụ trách CNTT của xã cần thường xuyên theo dõi, kiểm tra các bản ghi nhật ký và sự kiện hệ thống để phát hiện các dấu hiệu bất thường hoặc nguy cơ mất an toàn, kịp thời báo cáo lãnh đạo để có biện pháp xử lý

Điều 8. Quản lý tài khoản và quyền truy cập

1. Mỗi cán bộ, công chức được cấp tài khoản riêng biệt (định danh duy nhất) để sử dụng các hệ thống thông tin của UBND xã, tương ứng với công việc được giao. Không sử dụng chung tài khoản giữa nhiều người. Khi người dùng có sự thay đổi (điều chuyển công tác, nghỉ việc, nghỉ hưu), trong vòng 05 ngày làm việc kể từ khi có quyết định, bộ phận tổ chức của UBND xã phải thông báo bằng văn bản cho đơn vị quản trị hệ thống thông tin để điều chỉnh hoặc thu hồi, hủy bỏ các quyền truy cập của người đó.

2. Người sử dụng phải đặt mật khẩu mạnh cho các tài khoản được cấp. Khuyến cáo mật khẩu tối thiểu 8 ký tự, bao gồm chữ hoa, chữ thường, chữ số và ký tự đặc biệt. Định kỳ ít nhất 03 tháng một lần phải thay đổi mật khẩu truy cập hệ thống. Không chia sẻ mật khẩu cho bất kỳ ai; không sử dụng một mật khẩu cho nhiều hệ thống khác nhau. Nếu nghi ngờ mật khẩu bị lộ, phải đổi ngay mật khẩu và báo cho quản trị hệ thống. Các tài khoản cần được thiết lập cơ chế khóa tạm thời nếu đăng nhập sai mật khẩu quá một số lần quy định (ví dụ 5 lần liên tiếp).

3. Phân quyền truy cập: Quyền truy cập vào các hệ thống, cơ sở dữ liệu được phân công theo đúng chức năng, nhiệm vụ của từng cá nhân. Chỉ cấp quyền ở mức tối thiểu cần thiết để hoàn thành công việc. Những tác vụ quan trọng (như phê duyệt hồ sơ trên cổng dịch vụ công, xóa dữ liệu, tạo người dùng mới…) phải được thực hiện bởi người có thẩm quyền được phân công.

4. Tài khoản quản trị hệ thống (quản trị mạng, quản trị máy chủ, quản trị cơ sở dữ liệu, quản trị ứng dụng) phải được tách biệt với tài khoản người dùng thông thường. Mỗi tài khoản quản trị chỉ giao cho đích danh một cá nhân quản trị, hạn chế tối đa

việc dùng chung tài khoản quản trị. Trường hợp buộc phải dùng chung (ví dụ tài khoản "admin" mặc định không thể tách) thì phải được lãnh đạo cho phép bằng văn bản, và có giải pháp ghi lại lịch sử thao tác để xác định trách nhiệm từng cá nhân khi sử dụng. Kích hoạt các cơ chế kiểm soát đặc biệt với tài khoản quản trị: ví dụ thiết lập xác thực hai yếu tố (2FA) nếu có khả năng, tự động đăng xuất nếu phiên làm việc không hoạt động trong một thời gian ngắn, hạn chế phạm vi IP được phép truy cập bằng tài khoản quản trị.

5. UBND xã xây dựng hoặc tuân thủ các quy định/quy trình quản lý tài khoản người dùng cho từng hệ thống thông tin. Nội dung bao gồm: quy trình cấp mới tài khoản (có phê duyệt của lãnh đạo), quy trình thay đổi, hủy bỏ tài khoản khi người dùng thôi nhiệm vụ; quản lý mật khẩu mặc định khi cài đặt hệ thống (phải đổi ngay mật khẩu mặc định khi triển khai); và quy định kiểm tra, rà soát định kỳ danh sách tài khoản người dùng trên các hệ thống để kịp thời phát hiện tài khoản không sử dụng hoặc cấp quyền quá mức.

Điều 9. An toàn trong sử dụng máy tính và ứng dụng phần mềm

1. Mỗi cán bộ, công chức phải có trách nhiệm bảo đảm an toàn cho máy tính được giao phục vụ công việc. Chỉ cài đặt phần mềm hợp lệ, có bản quyền hoặc nguồn gốc rõ ràng cho công việc; không tự ý cài thêm hoặc gỡ bỏ phần mềm trên máy tính của cơ quan nếu chưa được sự đồng ý của bộ phận phụ trách CNTT. Hệ điều hành và các phần mềm trên máy tính cần được cập nhật thường xuyên (cập nhật các bản vá bảo mật) khi có phiên bản mới.

2. Tất cả máy tính phải được cài đặt và luôn mở phần mềm diệt virus/anti-malware có bản quyền, thiết lập chế độ cập nhật tự động cơ sở dữ liệu virus hàng ngày. Định kỳ hoặc trước khi sử dụng, quét virus đối với các thiết bị lưu trữ dữ liệu mang từ bên ngoài vào hệ thống. Không mở các email, tệp tin đính kèm hoặc đường link lạ nếu nghi ngờ nguồn gốc không đáng tin cậy, để tránh nhiễm mã độc. Nếu phát hiện dấu hiệu máy nhiễm mã độc (ví dụ chạy chậm bất thường, có hành vi lạ), cần ngắt kết nối mạng, tạm tắt máy và báo ngay cho cán bộ phụ trách CNTT để xử lý.

3. Chỉ truy cập các trang thông tin điện tử, ứng dụng trực tuyến tin cậy, phục vụ cho công việc chuyên môn hoặc mục đích được phép. Không truy cập các trang web có nội dung không liên quan nhiệm vụ, hoặc các trang có dấu hiệu không an toàn (như trang web lừa đảo, cờ bạc, web đen, v.v.). Tuyệt đối không sử dụng máy tính của cơ quan để thực hiện hành vi tấn công, xâm nhập trái phép vào hệ thống khác trên mạng.

4. Người sử dụng có trách nhiệm bảo mật tài khoản và thông tin cá nhân của mình. Không tiết lộ thông tin đăng nhập (tên người dùng, mật khẩu) cho người khác; không lưu trữ mật khẩu ở nơi dễ bị phát hiện (như giấy nhớ dán trên màn hình). Đăng

xuất khỏi các hệ thống ứng dụng khi không sử dụng. Khóa màn hình máy tính khi rời khỏi chỗ làm việc dù trong thời gian ngắn, để tránh người khác lợi dụng truy cập. Hết giờ làm việc nên tắt máy tính và các thiết bị để tiết kiệm năng lượng và phòng tránh truy cập trái phép.

5. Hạn chế việc chia sẻ nội dung, tài nguyên cục bộ trên từng máy tính cá nhân. Nếu cần chia sẻ tệp tin, dữ liệu cho đồng nghiệp, nên sử dụng thư mục dùng chung trên máy chủ nội bộ đã được thiết lập phân quyền, thay vì mở chia sẻ từ máy cá nhân. Trường hợp bắt buộc phải chia sẻ thư mục/tệp tin từ máy cá nhân, phải thiết lập mật khẩu cho việc truy cập vào tài nguyên chia sẻ đó, và gỡ bỏ chia sẻ ngay khi không còn cần thiết.

6. Không tự ý kết nối các thiết bị ngoại vi không tin cậy vào máy tính của cơ quan (ví dụ: USB không rõ nguồn gốc, thiết bị lưu trữ của người lạ) để tránh nguy cơ lây nhiễm mã độc. Các thiết bị cá nhân (điện thoại, laptop cá nhân) không nên kết nối vào mạng nội bộ hoặc cổng USB của máy tính cơ quan nếu không thực sự cần thiết và chưa được quét virus.

7. Sử dụng chữ ký số: UBND xã khuyến khích và yêu cầu (đối với các lĩnh vực bắt buộc) ứng dụng chữ ký số chuyên dùng cho cán bộ lãnh đạo, cán bộ phụ trách trong trao đổi văn bản điện tử và dịch vụ công trực tuyến. Việc sử dụng chữ ký số giúp đảm bảo tính xác thực và toàn vẹn của văn bản điện tử, phòng chống giả mạo và nâng cao an ninh thông tin trong giao dịch điện tử.

Điều 10. Đảm bảo an toàn cho các hệ thống ứng dụng đặc thù

1. Đối với phần mềm quản lý văn bản điều hành: Đây là hệ thống thông tin quan trọng hỗ trợ công tác chỉ đạo, điều hành của UBND xã. Cần thực hiện các biện pháp:

a) Quản lý chặt chẽ tài khoản người dùng: Cấp tài khoản cho cán bộ đúng phạm vi chức năng, phân quyền theo vị trí công tác (ví dụ: quyền xem, quyền tạo văn bản, quyền phê duyệt…) trên phần mềm. Thu hồi hoặc tạm khóa tài khoản ngay khi cán bộ chuyển công tác hoặc nghỉ việc, đảm bảo không tồn tại tài khoản "dư thừa".

b) Xác thực và chữ ký số: Cán bộ lãnh đạo xã, văn thư, và các đối tượng được phân quyền ký số văn bản phải sử dụng chứng thư số được cấp để ký số trên hệ thống quản lý văn bản. Kiểm tra tính hợp lệ của chữ ký số và dấu thời gian khi nhận văn bản đến.

c) Sao lưu dữ liệu: Thực hiện sao lưu định kỳ cơ sở dữ liệu của hệ thống quản lý văn bản (ví dụ hàng ngày hoặc hàng tuần tùy theo tần suất xử lý văn bản). Bản sao lưu cần được lưu trên thiết bị lưu trữ an toàn, tách biệt khỏi hệ thống chính (ví dụ lưu lên máy chủ dự phòng hoặc thiết bị lưu trữ rời) để phòng trường hợp hệ thống gặp sự cố.

d) Bảo mật nội dung: Tuân thủ quy định phân loại và bảo mật đối với văn bản tài liệu trên hệ thống. Những văn bản nội bộ hoặc tài liệu mật không đưa lên hệ thống nếu hệ thống không được thiết kế cho nội dung mật. Áp dụng tính năng đặt mật khẩu hoặc phân quyền hạn chế đối với tài liệu chứa thông tin nhạy cảm nếu phần mềm hỗ trợ.

đ) Đối với hệ thống camera giám sát: Hệ thống camera an ninh do UBND xã quản lý (tại trụ sở UBND xã hoặc trên địa bàn xã nếu có) phải được vận hành theo đúng quy định về an ninh mạng. Chỉ sử dụng các loại camera giám sát đáp ứng yêu cầu an toàn thông tin mạng theo tiêu chuẩn, có nguồn gốc xuất xứ rõ ràng, sản phẩm chính hãng chất lượng. Không sử dụng camera trôi nổi không có chứng nhận chất lượng, hoặc các camera đã được cơ quan chức năng cảnh báo về lỗ hổng bảo mật.

e) Thay đổi mật khẩu mặc định của camera ngay khi lắp đặt. Thiết lập tài khoản quản trị camera với mật khẩu mạnh; tắt các tài khoản/ dịch vụ không cần thiết trên camera. Cập nhật firmware cho camera lên phiên bản mới do nhà sản xuất cung cấp để vá các lỗ hổng (nếu có).

f) Đặt hệ thống camera trong một mạng riêng tách biệt với mạng máy tính văn phòng. Nếu camera có kết nối Internet (để xem từ xa), phải cấu hình cổng truy cập, địa chỉ IP tĩnh và sử dụng các biện pháp mã hóa, xác thực hai lớp (VPN, xác thực qua đám mây có bảo mật) để ngăn ngừa truy cập trái phép. Xem xét giới hạn phạm vi truy cập từ xa.

g) Phân công bộ phận thường xuyên theo dõi hình ảnh và trạng thái hoạt động của hệ thống camera. Nếu phát hiện dấu hiệu camera bị truy cập trái phép (ví dụ xoay camera bất thường, cấu hình bị thay đổi đột ngột, camera tự khởi động lại nhiều lần…), phải ngắt kết nối và kiểm tra ngay. Thông báo kịp thời cho cơ quan chuyên môn nếu nghi ngờ camera bị tấn công để phối hợp xử lý.Dữ liệu ghi hình của camera (nếu được lưu trữ) phải được bảo vệ, chỉ những người có nhiệm vụ mới được trích xuất, xem. Tuân thủ quy định pháp luật về bảo vệ đời tư nếu camera ghi hình tại nơi công cộng.

2. Đối với Cổng dịch vụ công và Trang thông tin điện tử của xã:

a) Quản lý nội dung và tài khoản: Phân công cán bộ quản trị cổng/trang thông tin điện tử của xã. Tài khoản quản trị nội dung phải được bảo mật cao (mật khẩu mạnh, đổi định kỳ tương tự quy định tại Điều 7). Khi đăng tải thông tin, phải tuân thủ quy chế phát ngôn, không để lộ thông tin nhạy cảm, không đăng tải nội dung ngoài phạm vi cho phép.

b) Giám sát an ninh web: Thường xuyên kiểm tra các biểu hiện bất thường trên website (như nội dung bị thay đổi không do quản trị viên thực hiện, hiệu năng hệ thống chậm bất thường có thể do tấn công). Phối hợp với đơn vị quản trị cấp trên (nếu có) để cập nhật các bản vá bảo mật cho hệ quản trị nội dung (CMS) của trang web.

Điều 11. Phối hợp với các cơ quan chức năng về an toàn, an ninh mạng

1. UBND xã phân công Văn phòng HĐND & UBND xã làm đầu mối liên hệ với các cơ quan có thẩm quyền cấp trên về an toàn thông tin tại hệ thống thông tin của UBND xã. Cụ thể, đầu mối này có trách nhiệm phối hợp chặt chẽ với Công an xã (cơ quan phụ trách quản lý nhà nước về ATTT, an ninh mạng), Đội ứng cứu sự cố an toàn thông tin mạng thành phố và Sở Khoa học và Công nghệ thành phố Hà Nội trong việc triển khai các hoạt động bảo đảm ATTT cho các hệ thống thông tin của xã.

- Phối hợp Công an Thành phố thực hiện công tác tập huấn, tuyên truyền nâng cao nhận thức về bảo đảm an ninh mạng, an toàn thông tin cho cán bộ, công chức, viên chức, người lao động thuộc xã.

2. Đầu mối ATTT của xã có nhiệm vụ tiếp nhận và xử lý các cảnh báo, sự cố ATTT do các cơ quan chuyên trách thông báo; đồng thời chủ động tham gia các chương trình, hoạt động về an toàn thông tin do cấp trên tổ chức (ví dụ: các đợt diễn tập ứng cứu sự cố mạng, các khóa tập huấn, hội nghị về an ninh mạng).

- Ngoài ra, tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của Công an Thành phố.

3. UBND xã và các cá nhân liên quan có trách nhiệm phối hợp, cung cấp thông tin và tạo điều kiện thuận lợi cho các cơ quan chức năng (Công an, Sở KHCN, Thanh tra chuyên ngành…) khi tiến hành kiểm tra, điều tra, khắc phục sự cố về an toàn thông tin mạng tại đơn vị. Phối hợp chặt chẽ với lực lượng Công an trong công tác phòng ngừa, phát hiện và ngăn chặn các hành vi tấn công, xâm phạm ATTT trên địa bàn xã.

- Ngoài ra, thường xuyên phối hợp với Công an thành phố trong công tác bảo đảm an ninh mạng, an toàn thông tin tại UBND xã.

Điều 12. Ứng cứu và xử lý sự cố an toàn thông tin

1. Khi xảy ra sự cố hoặc phát hiện nguy cơ mất an toàn thông tin, phải thực hiện theo nguyên tắc kịp thời, nhanh chóng, đồng bộ và hiệu quả; ưu tiên sử dụng lực lượng và phương tiện tại chỗ để xử lý bước đầu, đồng thời báo cáo cấp trên và yêu cầu hỗ trợ khi vượt quá khả năng. Đảm bảo tuân thủ các quy định pháp luật về điều phối ứng cứu sự cố và bảo vệ thông tin cá nhân, bí mật riêng tư trong quá trình xử lý.

2. Phân loại mức độ sự cố: UBND xã cần quy định việc đánh giá sơ bộ mức độ nghiêm trọng của sự cố để có biện pháp xử lý phù hợp. Ví dụ: Mức thấp – sự cố ảnh hưởng rất hạn chế, không làm gián đoạn hoạt động; Mức trung bình – sự cố ảnh hưởng một phần nhưng không đình trệ hoàn toàn công việc; Mức cao – sự cố gây tê liệt một phần quan trọng của hệ thống, ảnh hưởng lớn; Mức khẩn cấp – sự cố nghiêm trọng làm đình trệ hầu hết hoạt động chính của đơn vị.

- Quy trình ứng cứu: Khi phát hiện hoặc được thông báo về sự cố:

Bước 1: Xử lý tức thời tại chỗ: Cán bộ kỹ thuật tại xã phải nhanh chóng áp dụng các biện pháp để cô lập và ngăn chặn sự cố lan rộng (ví dụ: cách ly máy tính bị nhiễm virus ra khỏi mạng, khóa tài khoản bị tấn công, chuyển dịch vụ sang hệ thống dự phòng…). Đồng thời ghi nhận các thông tin ban đầu về sự cố (thời gian, hiện tượng, đối tượng ảnh hưởng, v.v.).

Bước 2: Báo cáo lãnh đạo và cấp trên: Lãnh đạo UBND xã phải được báo cáo ngay. Đối với sự cố nghiêm trọng ở mức cao hoặc khẩn cấp, hoặc sự cố vượt quá khả năng khắc phục của xã, lãnh đạo UBND xã báo cáo ngay lên UBND cấp trên (UBND Thành phố …),CATP và Sở Khoa học và Công nghệ TP Hà Nội để được hướng dẫn, hỗ trợ xử lý kịp thời.

Bước 3: Hỗ trợ và khắc phục: Phối hợp với các cơ quan chức năng (đội ứng cứu sự cố của Thành phố, cơ quan công an nếu có dấu hiệu tấn công hình sự) để điều tra nguyên nhân, khắc phục triệt để sự cố. Cung cấp đầy đủ, chính xác thông tin cần thiết cho cơ quan cấp trên khi được yêu cầu. Thực hiện theo đúng hướng dẫn của chuyên gia/cơ quan cấp trên trong quá trình xử lý.

Bước 4: Báo cáo kết quả: Sau khi sự cố được xử lý, UBND xã lập báo cáo bằng văn bản gửi cấp trên và các cơ quan quản lý nhà nước liên quan, nêu rõ diễn biến, nguyên nhân, biện pháp khắc phục và thiệt hại (nếu có). Đồng thời rút kinh nghiệm và đề ra biện pháp phòng ngừa sự cố tương tự trong tương lai.

3. UBND xã công bố thông tin liên hệ đầu mối tiếp nhận thông báo sự cố an toàn thông tin (họ tên cán bộ phụ trách, số điện thoại, email) trên trang thông tin điện tử của xã. Khi có thay đổi về đầu mối liên hệ, phải cập nhật kịp thời và thông báo cho Sở Khoa học và Công nghệ để tổng hợp.

- Ngoài ra, thường xuyên phối hợp với Công an thành phố trong công tác bảo đảm an ninh mạng, an toàn thông tin, khắc phục, xử lý sự cố tại đơn vị UBND xã.

4. Trách nhiệm của cán bộ, nhân viên: Mọi cán bộ, công chức, người lao động và cả bên thứ ba khi phát hiện hoặc nghi ngờ có sự cố ATTT đối với hệ thống của xã, đều phải báo cáo ngay cho người phụ trách hoặc lãnh đạo đơn vị. Việc báo sớm giúp ngăn chặn, giảm thiểu thiệt hại do sự cố gây ra. Không được che giấu sự cố hoặc chậm trễ báo cáo vì bất kỳ lý do gì.

5. Định kỳ, UBND xã nên phối hợp với cơ quan chuyên môn tổ chức diễn tập ứng cứu sự cố ở quy mô phù hợp (ví dụ: diễn tập xử lý tình huống máy tính nhiễm mã độc tống tiền, diễn tập khi website bị tấn công từ chối dịch vụ…) nhằm nâng cao kỹ năng ứng phó cho đội ngũ cán bộ kỹ thuật và lãnh đạo. Cập nhật, bổ sung phương án ứng cứu sự cố của xã sau mỗi lần diễn tập hoặc sau các sự cố thực tế để ngày càng hoàn thiện.

Chương III
TỔ CHỨC THỰC HIỆN

Điều 13. Trách nhiệm của UBND xã

1. Chủ tịch UBND xã chịu trách nhiệm cao nhất về công tác bảo đảm an ninh mạng, an toàn thông tin tại đơn vị mình. Nếu để xảy ra các vụ việc mất an toàn thông tin nghiêm trọng do lơ là, thiếu trách nhiệm, Chủ tịch UBND xã sẽ chịu trách nhiệm trước UBND cấp trên theo quy định.

2. Chủ tịch UBND xã trực tiếp hoặc phân công PHÓ CHỦ TỊCH UBND xã có trách nhiệm tổ chức triển khai thực hiện đầy đủ các quy định tại Quy chế này trong phạm vi xã. Ban hành các văn bản, nội quy nội bộ cần thiết để cụ thể hóa và thực thi các biện pháp bảo đảm ATTT phù hợp với tình hình thực tế xã (ví dụ: quy định về quản lý tài khoản, quy trình sao lưu dữ liệu, quy trình báo cáo sự cố…)

3. Đảm bảo bố trí nguồn kinh phí thích đáng cho công tác bảo đảm an ninh, an toàn thông tin. Tỷ lệ chi cho sản phẩm, dịch vụ ATTT tối thiểu 10% trên tổng kinh phí chi cho công nghệ thông tin, chuyển đổi số hàng năm và trong các dự án CNTT của xã.

4. Kế hoạch ngân sách hàng năm cần có mục riêng cho hoạt động ATTT (mua sắm giải pháp bảo mật, thuê dịch vụ an toàn thông tin, đào tạo nhân lực…).

5. Phân công nhân sự: Chỉ đạo phân công ít nhất một cán bộ chuyên trách hoặc kiêm nhiệm về an toàn thông tin của UBND xã. Tạo điều kiện để cán bộ này được tham gia các khóa đào tạo, bồi dưỡng nâng cao trình độ về an toàn thông tin. Trường hợp cần thiết, đề xuất thành lập tổ công tác về ATTT của xã, gồm các thành viên của Văn phòng, Văn hóa - Xã hội, Công an xã … để phối hợp triển khai nhiệm vụ đảm bảo ATTT.

- Chức năng, nhiệm vụ của Văn Phòng HĐND & UBND thuộc xã Phúc Lộc, trong đó bao gồm cán bộ chuyên trách công nghệ thông tin trực thuộc Văn Phòng HĐND & UBND xã Phúc Lộc

a) Chịu trách nhiệm bảo đảm ATTTM của đơn vị;

b) Tham mưu lãnh đạo cơ quan ban hành các quy chế, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm ATTTM;

c) Thực hiện việc giám sát, đánh giá, báo cáo lãnh đạo cơ quan các rủi ro mất an toàn thông tin và mức độ nghiêm trọng của các rủi ro đó;

d) Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố ATTTM;

đ) Thường xuyên cập nhật nâng cao kiến thức, trình độ chuyên môn đáp ứng yêu cầu bảo đảm ATTTM của đơn vị

- Phối hợp Công an Thành phố thực hiện công tác tập huấn, tuyên truyền nâng cao nhận thức về bảo đảm an ninh mạng, an toàn thông tin cho cán bộ, công chức, viên chức, người lao động thuộc xã.

6. Chỉ đạo tổ chức các buổi tập huấn, tuyên truyền cho toàn thể cán bộ, công chức của xã về kiến thức, kỹ năng bảo đảm an toàn thông tin. Lồng ghép nội dung phổ biến quy định ATTT trong các cuộc họp định kỳ của cơ quan. Khuyến khích cán bộ tham gia các chương trình đào tạo, hội thảo về ATTT do thành phố tổ chức, đồng thời phối hợp với Công an Thành phố (CATP) và Sở Khoa học và Công nghệ Thành phố Hà Nội trong công tác đào tạo, hướng dẫn nhằm nâng cao nhận thức và kỹ năng phòng, chống nguy cơ mất an toàn thông tin. Phối hợp Công an Thành phố thực hiện công tác tập huấn, tuyên truyền nâng cao nhận thức về bảo đảm an ninh mạng, an toàn thông tin cho cán bộ, công chức, viên chức, người lao động thuộc xã.

7. Chủ tịch UBND xã trực tiếp hoặc phân công PHÓ CHỦ TỊCH UBND xã chỉ đạo thực hiện việc tự kiểm tra, đánh giá định kỳ hàng năm về tình hình an ninh mạng, an toàn thông tin tại đơn vị. Có thể lập đoàn kiểm tra nội bộ hoặc yêu cầu bộ phận chuyên trách CNTT tiến hành đánh giá, báo cáo lãnh đạo về các rủi ro, điểm yếu và mức độ tuân thủ các quy định ATTT trong cơ quan.

Điều 14. Trách nhiệm của cán bộ phụ trách an toàn thông tin

Cán bộ được giao phụ trách an toàn thông tin của UBND xã có trách nhiệm:

1. Chủ động tham mưu cho lãnh đạo UBND xã ban hành các quy chế, quy trình nội bộ về bảo đảm ATTT; đề xuất triển khai các giải pháp kỹ thuật, dự án đầu tư về ATTT khi cần thiết.

2. Thực hiện hoặc phối hợp thực hiện công tác quản trị, giám sát an toàn thông tin trên các hệ thống của xã. Theo dõi, kiểm tra đánh giá rủi ro mất an toàn thông tin và mức độ nghiêm trọng, báo cáo kịp thời cho lãnh đạo để có biện pháp xử lý. Thường xuyên kiểm tra việc tuân thủ các quy định ATTT của người dùng; phát hiện và ngăn chặn kịp thời các truy cập, hành vi trái phép.

3. Đóng vai trò đầu mối kỹ thuật trong ứng cứu, xử lý sự cố ATTT tại xã. Phối hợp với các cá nhân, đơn vị liên quan trong việc kiểm soát, khắc phục sự cố. Khi xảy ra sự cố, phải có mặt kịp thời (trực tiếp hoặc từ xa) để xử lý ban đầu, đồng thời liên hệ các đội ứng cứu sự cố cấp trên để hỗ trợ nếu cần.

4. Đảm bảo việc tạo lập, thay đổi, hủy tài khoản người dùng trên các hệ thống tuân theo đúng quy trình và được phê duyệt. Thiết lập cơ chế phân quyền chặt chẽ, đúng nguyên tắc; thường xuyên rà soát phát hiện các tài khoản không sử dụng hoặc có dấu hiệu bất thường.

5. Giám sát việc vận hành an toàn các thiết bị mạng, máy chủ, máy trạm; cập nhật bản vá cho hệ điều hành, ứng dụng kịp thời khi có bản vá bảo mật mới. Đảm bảo các cấu hình bảo mật (tường lửa, antivirus…) được duy trì hoạt động hiệu quả.

6. Tổng hợp và báo cáo định kỳ theo yêu cầu: xây dựng báo cáo hàng năm về tình hình an toàn thông tin của xã (theo biểu mẫu của thành phố nếu có) gửi về UBND thành phố Hà Nội (qua Sở Khoa học và Công nghệ) trước ngày 15/01 hàng năm; báo cáo đột xuất khi có sự cố nghiêm trọng; cung cấp thông tin về tiến độ xây dựng, thẩm định hồ sơ xác định cấp độ hệ thống thông tin về cơ quan cấp trên theo quy định (ví dụ báo cáo hàng tháng nếu được yêu cầu)

7. Thường xuyên cập nhật kiến thức, nâng cao trình độ chuyên môn về CNTT và ATTT. Tự nghiên cứu, học tập cũng như tham gia các khóa đào tạo, hội thảo chuyên ngành về an toàn thông tin khi có điều kiện, nhằm đáp ứng yêu cầu ngày càng cao trong công tác bảo đảm ATTT của đơn vị.

Điều 15. Trách nhiệm của cán bộ, công chức và người lao động trong UBND xã

1. Mọi cán bộ, công chức, viên chức và người lao động tại UBND xã phải nghiêm túc chấp hành Quy chế này, các quy định nội bộ liên quan cũng như các quy định pháp luật về an toàn thông tin. Mỗi cá nhân chịu trách nhiệm bảo đảm an ninh, an toàn thông tin trong phạm vi công việc và quyền hạn được giao.

2. Mỗi cá nhân phải có trách nhiệm quản lý, bảo quản thiết bị CNTT được giao (máy tính, điện thoại công vụ, USB, v.v.) và bảo mật tài khoản truy cập của mình. Không tiết lộ mật khẩu, không cho người không có thẩm quyền mượn thiết bị hoặc sử dụng tài khoản của mình. Chỉ sử dụng thiết bị và tài khoản vào mục đích công việc được giao; chịu trách nhiệm nếu để xảy ra mất ATTT do lỗi cá nhân (ví dụ: do lộ mật khẩu, do tải phần mềm trái phép gây nhiễm mã độc…)

3. Khi phát hiện bất kỳ dấu hiệu nguy cơ hoặc sự cố mất an toàn thông tin (như máy tính nhiễm virus, phát hiện lỗ hổng, bị mất thiết bị lưu trữ chứa dữ liệu, …), phải báo cáo ngay cho cấp trên trực tiếp và cán bộ phụ trách CNTT của xã. Thời gian báo cáo tính từ khi phát hiện sự cố phải sớm nhất có thể, ưu tiên thông tin trực tiếp (gọi điện, nhắn tin) đến người phụ trách để kịp thời xử lý.

4. Cán bộ, công chức và người lao động cần tham gia đầy đủ các chương trình đào tạo, tập huấn về an toàn thông tin do cơ quan hoặc cấp trên tổ chức. Nghiêm túc tự rèn luyện kỹ năng, nâng cao nhận thức về các mối đe dọa an ninh mạng (như nhận biết email lừa đảo, cách đặt mật khẩu an toàn, sử dụng mạng xã hội an toàn…).

5. Cá nhân vi phạm các quy định về bảo đảm an ninh, an toàn thông tin của UBND xã, tùy mức độ, sẽ bị xem xét xử lý kỷ luật theo quy định của pháp luật và nội quy cơ quan. Nếu hành vi vi phạm gây hậu quả nghiêm trọng (như làm lộ bí mật nhà nước, gây thiệt hại lớn về kinh tế…), có thể bị truy cứu trách nhiệm hành chính hoặc hình sự theo quy định hiện hành.

Chương IV
ĐIỀU KHOẢN THI HÀNH

Điều 16. Hiệu lực thi hành

Quy chế này có hiệu lực kể từ ngày ký.

Điều 17. Tổ chức thực hiện

1. Các bộ phận, cá nhân thuộc UBND xã và các đơn vị liên quan có trách nhiệm thực hiện nghiêm túc các quy định tại Quy chế này. Định kỳ hàng năm, UBND xã tiến hành đánh giá tình hình thực hiện Quy chế, rút kinh nghiệm và cập nhật, sửa đổi bổ sung (nếu cần thiết) cho phù hợp với quy định cấp trên và thực tiễn mới phát sinh. Trong quá

trình thực hiện, nếu có vấn đề vướng mắc hoặc cần sửa đổi, bổ sung Quy chế, các đơn vị, cá nhân kịp thời phản ánh về UBND xã để tổng hợp, trình Chủ tịch UBND xã xem xét quyết định sửa đổi, bổ sung cho phù hợp./.

2. Văn phòng HĐND & UBND có trách nhiệm:

- Hằng năm lập kế hoạch đào tạo cho cán bộ, công chức, viên chức và người lao động để nâng cao kiến thức cơ bản và kỹ năng ATTTM.

- Tuyên truyền phổ biến, cập nhật các quy chế về an toàn thông tin để cán bộ hiểu rõ các quyền và trách nhiệm đối với công tác bảo đảm ATTTM.

- Phối hợp Công an Thành phố thực hiện công tác tập huấn, tuyên truyền nâng cao nhận thức về bảo đảm an ninh mạng, an toàn thông tin cho cán bộ, công chức, viên chức, người lao động thuộc xã.