ỦY BAN NHÂN DÂN XÃ PHƯỚC GIANG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 1653/QĐ-UBND	*Phước Giang, ngày 14 tháng 8 năm 2026*

QUYẾT ĐỊNH
Về việc ban hành Quy chế bảo đảm an toàn, an ninh mạng đối với Hệ thống thông tin Đảng ủy, HĐND, UBND xã Phước Giang

CHỦ TỊCH ỦY BAN NHÂN DÂN XÃ PHƯỚC GIANG

Căn cứ Luật Tổ chức chính quyền địa phương ngày 16/6/2025;

Căn cứ Luật An ninh mạng ngày 10/12/2025;

Căn cứ 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;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông về quy định chi tiết và hướng dẫn một số điều của 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;

Căn cứ Chỉ thị số 09/CT-TTg ngày 23/02/2024 của Thủ tướng Chính phủ về tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ;

Xét đề nghị của Trưởng phòng Văn hóa – Xã hội xã Phước Giang.

QUYẾT ĐỊNH

Điều 1. Ban hành kèm theo Quyết định này "Quy trình đối với Hệ thống thông tin Đảng ủy, HĐND, UBND xã Phước Giang", cụ thể gồm *(kèm theo quy trình)*:

1.1. Quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc;

1.2. Quy trình thử nghiệm và nghiệm thu hệ thống;

1.3. Quy trình quản lý an toàn mạng;

1.4. Quy trình quản lý an toàn máy chủ và ứng dụng;

1.5. Quy trình quản lý an toàn dữ liệu;

1.6. Quy trình quản lý sự cố an toàn thông tin;

1.7. Quy trình quản lý an toàn người sử dụng đầu cuối.

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

Điều 3. Chánh văn phòng HĐND và UBND, Trưởng phòng Văn hóa – Xã hội; Thủ trưởng các cơ quan, đơn vị và toàn thể cán bộ, công chức, viên chức các cơ quan Đảng, HĐND, UBND chịu trách nhiệm thi hành quyết định này./.

Nơi nhận:
- Như Điều 3;
- Lưu: VT.

CHỦ TỊCH

U.B.N.D XÃ PHƯỚC GIANG T. QUẢNG NGÃI

Nguyễn Văn Lễ

QUY TRÌNH
VÔ HIỆU HÓA TẤT CẢ CÁC QUYỀN RA, VÀO, TRUY CẬP TÀI NGUYÊN, QUẢN TRỊ HỆ THỐNG SAU KHI CÁN BỘ THÔI VIỆC

Quảng Ngãi - năm 2026

ỦY BAN NHÂN DÂN XÃ PHƯỚC GIANG

QUY TRÌNH

Vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc

	Người lập	Người xem xét	Người phê duyệt
Họ tên	Võ Thế Duy	Lê Viết Hiệp	Nguyễn Văn Lễ
Ký tên			
Chức vụ	Cán bộ phụ trách chuyển đổi số và ATTT - ANM	Chánh Văn phòng HĐND và UBND	Chủ tịch UBND
Ngày			

Số: 1653/QĐ-UBND Ngày ban hành: 14/8/2026

Quảng Ngãi - năm 2026

QUY TRÌNH

Vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc

1. Mục đích

Quy trình này nhằm quy định các bước vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc. Đảm bảo an toàn hệ thống thông tin, ngăn ngừa việc truy cập trái phép, rò rỉ dữ liệu hoặc lạm dụng tài nguyên của Đảng ủy, HĐND, UBND xã Phước Giang sau khi cán bộ, nhân viên hoặc người lao động thôi việc hoặc chấm dứt hợp đồng.

2. Phạm vi áp dụng

2.1 Đối tượng áp dụng

Áp dụng đối với toàn bộ hệ thống thông tin, phần mềm quản lý, hệ thống thư điện tử công vụ, mạng nội bộ (LAN, Wi-Fi), tài khoản hành chính, và các thiết bị CNTT của ĐẢNG ỦY, HĐND, UBND xã Phước Giang.

Đối tượng áp dụng: Toàn thể cán bộ, nhân viên, người lao động có quyền truy cập hệ thống thông tin ĐẢNG ỦY, HĐND, UBND xã Phước Giang.

2.2 Trách nhiệm áp dụng

Đơn vị / Bộ phận	Trách nhiệm chính
Phòng ban trực thuộc	Thông báo chính thức danh sách cán bộ thôi việc cho Văn phòng HĐND - UBND, Văn phòng Đảng Ủy tối thiểu 03 ngày trước khi chấm dứt hợp đồng.
Văn phòng HĐND - UBND, Văn phòng Đảng Ủy	Thực hiện vô hiệu hóa, thu hồi, xóa hoặc chuyển quyền truy cập trong toàn bộ hệ thống; lập biên bản xác nhận. Đối với các hệ thống do UBND tỉnh hoặc các Sở Ban Ngành cung cấp phân quyền thì Văn phòng HĐND – UBND tạo lập văn bản đề nghị đơn vị quản trị vô hiệu hóa, thu hồi, xóa hoặc chuyển quyền truy cập trong các hệ thống này.
Phòng ban trực thuộc	Kiểm tra, thu hồi tài liệu, thiết bị, tài khoản nội bộ của nhân viên thuộc phòng ban.
Người thôi việc	Bàn giao đầy đủ tài khoản, thiết bị, hồ sơ, dữ liệu theo quy định.

3. Định nghĩa, từ viết tắt

3.1 Định nghĩa

- *Admin*: Chánh Văn phòng HĐND - UBND, Văn phòng Đảng Ủy, người chịu trách nhiệm quản lý sự vận hành toàn bộ hệ thống mạng;

- *Hệ thống CNTT*: Toàn bộ cơ sở hạ tầng trang thiết bị CNTT, hệ thống phần cứng, phần mềm, CSDL thiết lập nên hệ thống CNTT cũng như hệ thống logic CNTT của ĐẢNG ỦY, HĐND, UBND xã Phước Giang;

- *Hệ thống Server:* Là hệ thống các máy chủ đặt tại phòng Server, từ đây hệ thống máy chủ các thiết bị mạng, được kết nối với nhau để thiết lập nên mạng logic vận hành hoạt động ổn định thông suốt trong toàn ĐẢNG ỦY, HĐND, UBND xã Phước Giang.

- *Mã nguồn:* Các mã nguồn phần mềm ứng dụng, website.

- *Sao lưu dữ liệu:* Là việc sao chép để lưu giữ dự phòng toàn bộ mã nguồn, dữ liệu lên một máy chủ lưu trữ dự phòng.

- *Phục hồi dữ liệu*: Là khi hệ thống có sự cố và bị mất dữ liệu, có thể dùng dữ liệu dự phòng để thay thế, phục hồi lại dữ liệu trên hệ thống.

- *Sao lưu tự động:* Là sẽ tự động sao lưu lại tất cả những dữ liệu mới được phát sinh theo lịch đã được lập. Tất cả dữ liệu được sao lưu tự động qua các bước sau:

+ Xác định dữ liệu cần sao lưu.

+ Đặt lịch sao lưu tự động.

+ Khai báo địa chỉ lưu dữ liệu.

+ Kiểm tra thường xuyên dữ liệu được sao lưu, đảm bảo dữ liệu sao lưu phải được toàn vẹn.

- *Phân loại dữ liệu:* Cơ sở dữ liệu, dữ liệu kế toán, dữ liệu văn bản, bản tính,....

3.2 Các từ viết tắt

- CNTT: Công nghệ thông tin

- HĐH: Hệ điều hành Windows, Linux.

4. Nội dung quy trình

4.1. Quy trình sao lưu

Bước 1: Tiếp nhận thông tin thôi việc

Khi có quyết định thôi việc hoặc tạm ngưng công tác, Phòng ban trực thuộc gửi thông báo chính thức bằng văn bản/email cho các Văn phòng HĐND - UBND, Văn phòng Đảng Ủy và các phòng liên quan.

Thông tin gồm: Họ tên, chức danh, ngày chấm dứt hợp đồng, danh sách hệ thống có quyền truy cập.

Bước 2: Xác định danh sách tài khoản và quyền truy cập

Văn phòng HĐND - UBND, Văn phòng Đảng Ủy rà soát toàn bộ hệ thống:

- Tài khoản miền (domain user) (nếu có).

- Tài khoản các phần mềm ứng dụng được cấp phát sử dụng

- Tài khoản thư điện tử công vụ.

- Tài khoản quản trị thiết bị mạng, hệ thống camera, cổng thông tin,… (Nếu có đối với Quản trị viên)

- Tài khoản truy cập từ xa (VPN, TeamViewer, AnyDesk, v.v.).

- Lập Danh sách tài khoản truy cập của cá nhân.

- ĐẢNG ỦY, HĐND, UBND xã Phước Giang hợp các hệ thống do UBND tỉnh hoặc các Sở Ban Ngành cung cấp tài khoản, phân quyền truy cập thì Văn phòng HĐND –

UBND tạo lập văn bản đề nghị đơn vị quản trị vô hiệu hóa, thu hồi, xóa hoặc chuyển quyền truy cập, ghi rõ thời điểm thực hiện trong các hệ thống này.

Bước 3: Thực hiện vô hiệu hóa quyền truy cập

Trong vòng 24 giờ kể từ thời điểm nhận thông báo chính thức, Văn phòng HĐND - UBND, Văn phòng Đảng Ủy phải:

- Khóa (disable) hoặc xóa tài khoản trên toàn bộ hệ thống.

- Gỡ quyền quản trị (admin) (nếu có).

- Thu hồi quyền truy cập khu vực mạng nội bộ.

- Ngắt quyền truy cập từ xa, hủy chứng chỉ bảo mật hoặc VPN key (nếu có).

- Đổi mật khẩu tài khoản dùng chung (nếu cá nhân từng được sử dụng).

- ĐẢNG ỦY, HĐND, UBND xã Phước Giang hợp các hệ thống do UBND tỉnh hoặc các Sở Ban Ngành cung cấp tài khoản, phân quyền truy cập thì Văn phòng HĐND – UBND xác nhân với đơn vị quản trị các hệ thống việc thực hiện các nội dung văn bản đề nghị vô hiệu hóa, thu hồi, xóa hoặc chuyển quyền truy cập trước đó.

Bước 4: Thu hồi thiết bị và dữ liệu

Trưởng các phòng ban trực thuộc phối hợp với Văn phòng HĐND - UBND, Văn phòng Đảng Ủy thu hồi các thiết bị, công cụ dụng cụ đã được cấp phát cho nhân sự như:

- Máy tính, điện thoại, USB, thẻ nhớ, thiết bị ngoại vi… (nếu có)

- Tài liệu, hồ sơ, phần mềm bản quyền, tài sản CNTT khác.

Kiểm tra và sao lưu dữ liệu công việc quan trọng trước khi xóa hoặc chuyển cho người kế nhiệm.

Văn phòng HĐND - UBND, Văn phòng Đảng Ủy xác minh không còn dữ liệu nhạy cảm được lưu trong thiết bị cá nhân.

Bước 5: Xác nhận và lưu hồ sơ

Sau khi hoàn tất, Văn phòng HĐND - UBND, Văn phòng Đảng Ủy lập Biên bản thu hồi và vô hiệu hóa quyền truy cập, có chữ ký của:

- Đại diện Văn phòng HĐND - UBND, Văn phòng Đảng Ủy;

- Phòng ban trực thuộc;

- Công chức, viên chức, người lao động thôi việc hoặc chuyển công tác;

Hồ sơ được lưu trữ tối thiểu 02 năm để phục vụ kiểm tra, tra soát.

Bước 6: Báo cáo người quản lý

Người được phân công sẽ lập báo cáo sau khi thực hiện quy trình.

5. Hiệu lực thi hành

Quy trình này có hiệu lực kể từ ngày ký và thay thế mọi hướng dẫn trước đây có nội dung tương tự. Văn phòng HĐND - UBND, Văn phòng Đảng Ủy chịu trách nhiệm hướng dẫn, kiểm tra và giám sát việc thực hiện. Ngoài ra, hàng quý Văn phòng HĐND - UBND, Văn phòng Đảng Ủy rà soát lại danh sách tài khoản đang hoạt động để đảm bảo không còn tài khoản của người đã thôi việc. Kết quả rà soát được báo cáo Lãnh đạo UBND.

QUY TRÌNH
THỬ NGHIỆM VÀ NGHIỆM THU HỆ THỐNG

Quảng Ngãi - năm 2026

ỦY BAN NHÂN DÂN XÃ PHƯỚC GIANG

QUY TRÌNH

Thử nghiệm và nghiệm thu hệ thống

	Người lập	Người xem xét	Người phê duyệt
Họ tên	Võ Thế Duy	Lê Viết Hiệp	Nguyễn Văn Lễ
Ký tên			
Chức vụ	Cán bộ phụ trách chuyển đổi số và ATTT - ANM	Chánh Văn phòng HĐND và UBND	Chủ tịch UBND
Ngày			

Số: 1653/QĐ-UBND Ngày ban hành: 14/8/2026

Quảng Ngãi - năm 2026

QUY TRÌNH
Thử nghiệm và nghiệm thu hệ thống

1. Mục đích

Đảm bảo tất cả các hệ thống công nghệ thông tin (CNTT) được triển khai, nâng cấp hoặc sửa đổi tại ĐẢNG ỦY, HĐND, UBND xã Phước Giang đều được kiểm tra, đánh giá kỹ lưỡng trước khi đưa vào vận hành chính thức, nhằm bảo đảm an toàn thông tin, tính ổn định, và đáp ứng đầy đủ yêu cầu nghiệp vụ.

2. Phạm vi áp dụng

2.1 Đối tượng áp dụng

Áp dụng cho toàn bộ quá trình:

- Cài đặt, nâng cấp, sửa đổi, hoặc triển khai mới các hệ thống CNTT, phần mềm, thiết bị mạng, máy chủ, hoặc cơ sở dữ liệu trong ĐẢNG ỦY, HĐND, UBND xã Phước Giang.

- Đối tượng thực hiện: Văn phòng HĐND - UBND, Văn phòng Đảng Ủy, Các phòng ban, nhà cung cấp dịch vụ hoặc nhà thầu kỹ thuật, và Ban Lãnh đạo.

2.2 Trách nhiệm áp dụng

Đơn vị / Bộ phận	Trách nhiệm chính
Văn phòng HĐND - UBND, Văn phòng Đảng Ủy	Chủ trì việc lập kế hoạch thử nghiệm, thực hiện kiểm tra kỹ thuật, bảo mật, và đánh giá vận hành.
Đơn vị sử dụng (Các phòng, ban)	Thực hiện thử nghiệm chức năng nghiệp vụ, ghi nhận kết quả, đề xuất điều chỉnh.
Nhà cung cấp / Đơn vị triển khai	Thực hiện cấu hình, hỗ trợ kỹ thuật, khắc phục lỗi phát sinh trong quá trình thử nghiệm.
Ban Lãnh đạo	Phê duyệt kế hoạch thử nghiệm, nghiệm thu kết quả và quyết định đưa hệ thống vào vận hành chính thức.

3. Định nghĩa, từ viết tắt

3.1 Định nghĩa

- *Admin:* Chánh Văn phòng HĐND - UBND, Văn phòng Đảng Ủy, người chịu trách nhiệm quản lý sự vận hành toàn bộ hệ thống mạng;

- *Hệ thống CNTT:* Toàn bộ cơ sở hạ tầng trang thiết bị CNTT, hệ thống phần cứng, phần mềm, CSDL thiết lập nên hệ thống CNTT cũng như hệ thống logic CNTT của ĐẢNG ỦY, HĐND, UBND xã Phước Giang;

- *Hệ thống Server:* Là hệ thống các máy chủ đặt tại phòng Sever, từ đây hệ thống máy chủ các thiết bị mạng, được kết nối với nhau để thiết lập nên mạng logic vận hành hoạt động ổn định thông suốt trong toàn ĐẢNG ỦY, HĐND, UBND xã Phước Giang.

- *Mã nguồn:* Các mã nguồn phần mềm ứng dụng, website.

- *Sao lưu dữ liệu:* Là việc sao chép để lưu giữ dự phòng toàn bộ mã nguồn, dữ liệu lên một máy chủ lưu dự phòng.

- *Phục hồi dữ liệu*: Là khi hệ thống có sự cố và bị mất dữ liệu, có thể dùng dữ liệu dự phòng để thay thế, phục hồi lại dữ liệu trên hệ thống.

- *Sao lưu tự động:* Là tự động sao lưu lại tất cả những dữ liệu mới được phát sinh theo lịch đã được lập. Tất cả dữ liệu được sao lưu tự động qua các bước sau:

+ Xác định dữ liệu cần sao lưu.

+ Đặt lịch sao lưu tự động.

+ Khai báo địa chỉ lưu dữ liệu.

+ Kiểm tra thường xuyên dữ liệu được sao lưu, đảm bảo dữ liệu sao lưu phải được toàn vẹn.

- *Phân loại dữ liệu:* Cơ sở dữ liệu, dữ liệu kế toán, dữ liệu văn bản, bản tính,....

3.2 Các từ viết tắt

* CNTT: Công nghệ thông tin

* HĐH: Hệ điều hành Windows, Linux.

4. Nội dung quy trình

Quy trình thử nghiệm và nghiệm thu hệ thống

Bước 1: Chuẩn bị và lập kế hoạch thử nghiệm

Văn phòng HĐND - UBND, Văn phòng Đảng Ủy phối hợp với đơn vị sử dụng lập Kế hoạch thử nghiệm hệ thống, bao gồm:

- Mục tiêu thử nghiệm;

- Phạm vi hệ thống, cấu hình phần cứng, phần mềm, mạng;

- Các tiêu chí đánh giá kỹ thuật, bảo mật, và hiệu năng;

- Phân công nhân sự tham gia;

- Thời gian và địa điểm thử nghiệm.

Kế hoạch được Tổ trưởng CNTT trình Ban Lãnh đạo phê duyệt.

Bước 2: Chuẩn bị môi trường thử nghiệm

Chuẩn bị môi trường thử nghiệm như sau:

- Thiết lập môi trường kiểm thử độc lập (test environment), tách biệt hoàn toàn khỏi hệ thống thật (production).

- Cài đặt phần mềm, cấu hình mạng, cơ sở dữ liệu theo đúng phiên bản, tài liệu kỹ thuật.

- Sao chép dữ liệu mẫu, dữ liệu giả lập (không dùng dữ liệu thật).

- Kiểm tra thiết bị, máy chủ, tài khoản, phân quyền thử nghiệm.

Bước 3: Thực hiện vô hiệu hóa quyền truy cập

Tiến hành thử nghiệm theo kịch bản kiểm thử (test case) đã xây dựng:

- Kiểm tra cài đặt và cấu hình.

- Kiểm tra các chức năng chính (đăng nhập, xử lý nghiệp vụ, in ấn, báo cáo).

- Thử nghiệm tải (load test) nếu là hệ thống nhiều người dùng.

- Thử nghiệm bảo mật (quyền truy cập, phân quyền, mã hóa, backup, logging).

- Kiểm tra khả năng tương thích với hệ thống hiện hữu.

Ghi nhận lỗi, sự cố, đề xuất khắc phục.

Bước 4: Tổng hợp kết quả và khắc phục

Văn phòng HĐND - UBND, Văn phòng Đảng Ủy lập Biên bản kết quả thử nghiệm, ghi rõ:

- Danh sách lỗi phát hiện;

- Mức độ ảnh hưởng (nghiêm trọng, trung bình, nhẹ);

- Biện pháp khắc phục;

- Trách nhiệm của nhà cung cấp hoặc bộ phận kỹ thuật.

Nhà cung cấp/đơn vị triển khai khắc phục lỗi, cập nhật lại hệ thống, và báo cáo hoàn thành.

Bước 5: Nghiệm thu hệ thống

Sau khi khắc phục, Văn phòng HĐND - UBND, Văn phòng Đảng Ủy tổ chức nghiệm thu với sự tham gia của:

- Đại diện Ban Lãnh đạo;

- Đại diện Văn phòng HĐND - UBND, Văn phòng Đảng Ủy;

- Đại diện Đơn vị sử dụng;

- Nhà cung cấp/triển khai.

Tiến hành:

- Kiểm tra vận hành thực tế;

- So sánh kết quả với tiêu chí trong kế hoạch thử nghiệm;

- Đánh giá an toàn bảo mật;

- Ký Biên bản nghiệm thu hệ thống.

Bước 6: Triển khai chính thức

Sau nghiệm thu, hệ thống được:

- Gắn mã định danh, cập nhật vào danh mục quản lý tài sản CNTT (nếu có);

- Giao quyền quản trị chính thức cho Văn phòng HĐND - UBND, Văn phòng Đảng Ủy;

- Lưu trữ toàn bộ hồ sơ kỹ thuật, nhật ký thử nghiệm, biên bản nghiệm thu.

Cập nhật hệ thống giám sát và sao lưu theo quy định an toàn thông tin.

Bước 7: Theo dõi sau triển khai chính thức

Phòng ban trực tiếp sử dụng phối hợp cán bộ được phân công CNTT theo dõi hoạt động hệ thống trong 30 ngày đầu sau khi vận hành chính thức.

Nếu phát sinh sự cố nghiêm trọng, có thể tạm ngưng hệ thống và kích hoạt quy trình "Xử lý sự cố an toàn thông tin".

Bước 8: Báo cáo người quản lý

Người được phân công sẽ lập báo cáo sau khi thực hiện báo cáo kết quả sau khi triển khai chính thức.

5. Hiệu lực và lưu trữ

Quy trình này có hiệu lực kể từ ngày ký.

Hồ sơ, biên bản và tài liệu liên quan được lưu tại Phòng ban trực tiếp sử dụng và cán bộ được phân công CNTT tối thiểu 05 năm.

Mọi thay đổi hoặc cập nhật quy trình phải được Lãnh đạo ĐẢNG ỦY, HĐND, UBND xã Phước Giang phê duyệt.

QUY TRÌNH
QUẢN LÝ AN TOÀN MẠNG

Quảng Ngãi - năm 2026

ỦY BAN NHÂN DÂN XÃ PHƯỚC GIANG

QUY TRÌNH
Quản lý an toàn mạng

	Người lập	Người xem xét	Người phê duyệt
Họ tên	Võ Thế Duy	Lê Viết Hiệp	Nguyễn Văn Lễ
Ký tên			
Chức vụ	Cán bộ phụ trách chuyển đổi số và ATTT - ANM	Chánh Văn phòng HĐND và UBND	Chủ tịch UBND
Ngày			

Số: 1653/QĐ-UBND Ngày ban hành: 14/8/2026

Quảng Ngãi - năm 2026

QUY TRÌNH

Quản lý an toàn mạng

1. Mục đích

Đảm bảo hệ thống mạng của ĐẢNG ỦY, HĐND, UBND xã Phước Giang (bao gồm mạng nội bộ, Internet, Wi-Fi, VPN, hệ thống camera, máy tính có kết nối mạng...) hoạt động ổn định, an toàn, hạn chế tối đa nguy cơ mất an toàn thông tin, rò rỉ dữ liệu hoặc tấn công mạng.

2. Phạm vị áp dụng

2.1 Đối tượng áp dụng

Áp dụng cho toàn bộ hệ thống mạng của ĐẢNG ỦY, HĐND, UBND xã Phước Giang: mạng LAN, Wi-Fi, VPN, mạng Internet, các hệ thống kết nối với hệ thống khác.

Đối tượng áp dụng: Văn phòng HĐND - UBND, Văn phòng Đảng Ủy, cán bộ kỹ thuật, các phòng ban trực thuộc và các đơn vị, tổ chức, nhà cung cấp dịch vụ, đơn vị bảo trì được cấp quyền truy cập hạ tầng mạng của ĐẢNG ỦY, HĐND, UBND xã Phước Giang.

2.2 Trách nhiệm áp dụng

Đơn vị / Bộ phận	Trách nhiệm chính
Văn phòng HĐND - UBND, Văn phòng Đảng Ủy	Quản lý, vận hành, giám sát và bảo mật toàn bộ hệ thống mạng.
Các phòng ban	Sử dụng hệ thống mạng theo đúng quy định, báo cáo kịp thời sự cố.
Nhà cung cấp dịch vụ / bảo trì thiết bị	Tuân thủ quy định bảo mật khi thực hiện bảo trì, không tự ý thay đổi cấu hình mạng.
Ban Lãnh đạo	Phê duyệt kế hoạch bảo trì, nâng cấp và xử lý các sự cố nghiêm trọng.

3. Định nghĩa, từ viết tắt

3.1. Định nghĩa

- *Admin*: Chánh Văn phòng HĐND - UBND, Văn phòng Đảng Ủy, người chịu trách nhiệm quản lý sự vận hành toàn bộ hệ thống mạng;

- *Hệ thống CNTT*: Toàn bộ cơ sở hạ tầng trang thiết bị CNTT, hệ thống phần cứng, phần mềm, CSDL thiết lập nên hệ thống CNTT cũng như hệ thống logic CNTT của ĐẢNG ỦY, HĐND, UBND xã Phước Giang;

- *Hệ thống Server:* Là hệ thống các máy chủ đặt tại phòng Server, từ đây hệ thống máy chủ các thiết bị mạng, được kết nối với nhau để thiết lập nên mạng logic vận hành hoạt động ổn định thông suốt trong toàn ĐẢNG ỦY, HĐND, UBND xã Phước Giang.

- *Mã nguồn:* Các mã nguồn phần mềm ứng dụng, website.

- *Sao lưu dữ liệu:* Là việc sao chép để lưu giữ dự phòng toàn bộ mã nguồn, dữ liệu lên một máy chủ lưu dự phòng.

- *Phục hồi dữ liệu*: Là khi hệ thống có sự cố và bị mất dữ liệu, có thể dùng dữ liệu dự phòng để thay thế, phục hồi lại dữ liệu trên hệ thống.

- *Sao lưu tự động:* Là tự động sao lưu lại tất cả những dữ liệu mới được phát sinh theo lịch đã được lập. Tất cả dữ liệu được sao lưu tự động qua các bước sau:

+ Xác định dữ liệu cần sao lưu.

+ Đặt lịch sao lưu tự động.

+ Khai báo địa chỉ lưu dữ liệu.

+ Kiểm tra thường xuyên dữ liệu được sao lưu, đảm bảo dữ liệu sao lưu phải được toàn vẹn.

- *Phân loại dữ liệu:* Cơ sở dữ liệu, dữ liệu kế toán, dữ liệu văn bản, bản tính,....

Các từ viết tắt

- CNTT: Công nghệ thông tin

- HĐH: Hệ điều hành Windows, Linux.

4. Nội dung quy trình

4.1. Quy trình quản lý an toàn mạng

Bước 1: Quản lý cấu trúc mạng

Văn phòng HĐND - UBND, Văn phòng Đảng Ủy lập sơ đồ mạng tổng thể (network diagram), bao gồm:

- Thiết bị mạng: router, switch, firewall, access point, modem, server...

- Kết nối liên mạng (Internet, VPN, DMZ, VLAN nội bộ).

- Hệ thống camera, máy chủ lưu trữ, máy tính, … kết nối mạng.

Cập nhật định kỳ mỗi 06 tháng hoặc khi có thay đổi hạ tầng.

Bước 2: Phân vùng và kiểm soát truy cập mạng

Văn phòng HĐND - UBND, Văn phòng Đảng Ủy thực hiện kiểm soát truy cập mạng như sau:

- Phân chia mạng thành các vùng chức năng riêng biệt theo hồ sơ thiết kế hệ thống.

- Áp dụng các chính sách trên thiết bị tường lửa (Firewall) bảo mật để kiểm soát luồng dữ liệu.

- Tất cả truy cập từ Internet vào hệ thống phải qua Firewall hoặc VPN được mã hóa.

Bước 3: Quản lý thiết bị và cấu hình

Thiết bị mạng phải có:

- Mật khẩu quản trị mạnh (theo quy định: ≥8 ký tự gồm chữ hoa, thường, số, ký tự đặc biệt).

- Cấu hình sao lưu định kỳ và lưu tại Phòng ban trực tiếp sử dụng phối hợp cán bộ được phân công CNTT (mã hóa nếu cần thiết).

- Ghi nhật ký cấu hình (change log) mỗi lần thay đổi.

Chỉ nhân viên CNTT được ủy quyền mới có quyền truy cập thiết bị mạng.

Khi bàn giao, thay đổi nhân sự, phải đổi toàn bộ mật khẩu quản trị thiết bị.

Bước 4: Giám sát an toàn mạng

Theo dõi:

- Lưu lượng mạng, truy cập bất thường.

- Các sự kiện cảnh báo từ firewall, antivirus, IDS.

- Tình trạng hoạt động của switch, router, access point.

Văn phòng HĐND - UBND, Văn phòng Đảng Ủy lập báo cáo sự cố mạng hàng tháng gửi Lãnh đạo ĐẢNG ỦY, HĐND, UBND xã Phước Giang.

Bước 5: Quản lý cập nhật và bảo trì

Cập nhật firmware và bản vá bảo mật cho thiết bị mạng ít nhất 2 lần/năm hoặc theo cảnh báo của nhà sản xuất.

Trước khi nâng cấp hệ thống mạng:

- Lập kế hoạch chi tiết.

- Thực hiện thử nghiệm trong môi trường mô phỏng trước khi nâng cấp.

- Có biên bản nghiệm thu sau bảo trì.

Bước 6: Quản lý truy cập từ xa (Remote Access)

Truy cập từ xa vào hệ thống mạng ĐẢNG ỦY, HĐND, UBND xã Phước Giang chỉ được phép qua:

- Tường lửa hoặc VPN có xác thực.

- Danh sách IP được cấp quyền truy cập.

Ghi nhật ký phiên làm việc (session log).

Chỉ được sử dụng phần mềm điều khiển từ xa khi cán bộ CNTT xác nhận (TeamViewer, AnyDesk, UltraViewer...).

Bước 7: Sao lưu và khôi phục hệ thống mạng

Sao lưu:

- Cấu hình thiết bị mạng, firewall, server.

- Dữ liệu nhật ký truy cập.

Lưu trữ ít nhất 02 bản sao lưu, trong đó 01 bản offline.

Định kỳ thử khôi phục cấu hình để đảm bảo tính sẵn sàng.

Bước 8: Xử lý sự cố và khôi phục sau sự cố

Khi phát hiện:

- Mất kết nối mạng diện rộng, nghi ngờ tấn công, rò rỉ dữ liệu → báo ngay cho cán bộ phụ trách CNTT và Văn phòng HĐND - UBND, Văn phòng Đảng Ủy.

- Văn phòng HĐND - UBND, Văn phòng Đảng Ủy và cán bộ phụ trách CNTT xác định nguyên nhân, cô lập vùng bị ảnh hưởng, ghi nhật ký sự cố.

- Báo cáo nhanh cho Ban Lãnh đạo và Cơ quan chuyên trách ATTT (nếu sự cố nghiêm trọng).

Sau khi xử lý, phải cập nhật báo cáo sự cố an toàn mạng.

Bước 9: Kiểm tra định kỳ

Thực hiện kiểm tra an toàn mạng hàng quý, bao gồm:

- Rà soát phân quyền truy cập.

- Quét lỗ hổng bảo mật (vulnerability scanning).

- Đánh giá nhật ký truy cập và sự kiện bất thường.

Báo cáo kết quả kiểm tra và kế hoạch khắc phục lên Lãnh đạo ĐẢNG ỦY, HĐND, UBND xã Phước Giang.

5. Hiệu lực thi hành

Quy trình này có hiệu lực kể từ ngày ký.

Văn phòng HĐND - UBND, Văn phòng Đảng Ủy chịu trách nhiệm phổ biến, giám sát và cập nhật định kỳ.

Hồ sơ, nhật ký, biên bản được lưu tối thiểu 05 năm.

QUY TRÌNH
QUẢN LÝ AN TOÀN MÁY CHỦ VÀ ỨNG DỤNG

Quảng Ngãi - năm 2026

ỦY BAN NHÂN DÂN XÃ PHƯỚC GIANG

QUY TRÌNH
Quản lý an toàn máy chủ và ứng dụng

	Người lập	Người xem xét	Người phê duyệt
Họ tên	Võ Thế Duy	Lê Viết Hiệp	Nguyễn Văn Lễ
Ký tên			
Chức vụ	Cán bộ phụ trách chuyển đổi số và ATTT - ANM	Chánh Văn phòng HĐND và UBND	Chủ tịch UBND
Ngày			

Số: 1653/QĐ-UBND Ngày ban hành: 14/8/2026

Quảng Ngãi - năm 2026

QUY TRÌNH
Quản lý an toàn máy chủ và ứng dụng

1. Mục đích

Đảm bảo toàn bộ hệ thống máy chủ, ứng dụng, cơ sở dữ liệu và dịch vụ CNTT của ĐẢNG ỦY, HĐND, UBND xã Phước Giang được quản lý, vận hành an toàn, tránh mất dữ liệu, gián đoạn dịch vụ hoặc bị tấn công xâm nhập.

2. Phạm vị áp dụng

2.1 đối tượng áp dụng

Áp dụng cho tất cả máy chủ vật lý, máy ảo, dịch vụ đám mây, ứng dụng nội bộ và hệ thống tích hợp:

- các hệ thống được cấp trên mua sắm tập trung và cấp quyền cho ĐẢNG ỦY, HĐND, UBND xã Phước Giang sử dụng

Áp dụng cho Văn phòng HĐND, UBND, văn phòng đảng ủy, cán bộ vận hành hệ thống, đơn vị phát triển phần mềm, nhà cung cấp bảo trì ứng dụng và các phòng ban trực tiếp sử dụng.

2.2 trách nhiệm áp dụng

Đơn vị / Bộ phận	Trách nhiệm chính
Cán bộ phụ trách CNTT Văn phòng HĐND - UBND, Văn phòng Đảng Ủy	Quản trị, giám sát, sao lưu vá lỗi và đảm bảo an toàn cho toàn bộ máy chủ & ứng dụng.
Nhà cung cấp phần mềm	Tuân thủ quy định bảo mật, không cài đặt hoặc thay đổi cấu hình khi chưa được phép.
Phòng ban trực tiếp sử dụng	Sử dụng ứng dụng đúng quy định, không cài đặt phần mềm trái phép, báo cáo sự cố ngay khi phát hiện.
Ban Lãnh đạo	Phê duyệt kế hoạch bảo trì, nâng cấp, và báo cáo sự cố nghiêm trọng.

3. Định nghĩa, từ viết tắt

3.1 Định nghĩa

- *Admin*: Chánh Văn phòng HĐND - UBND, Văn phòng Đảng Ủy, người chịu trách nhiệm quản lý sự vận hành toàn bộ hệ thống mạng;

- *Hệ thống CNTT*: Toàn bộ cơ sở hạ tầng trang thiết bị CNTT, hệ thống phần cứng, phần mềm, CSDL thiết lập nên hệ thống CNTT cũng như hệ thống logic CNTT của ĐẢNG ỦY, HĐND, UBND xã Phước Giang;

- *Hệ thống Server:* Là hệ thống các máy chủ đặt tại phòng Sever, từ đây hệ thống máy chủ các thiết bị mạng, được kết nối với nhau để thiết lập nên mạng logic vận hành hoạt động ổn định thông suốt trong toàn ĐẢNG ỦY, HĐND, UBND xã Phước Giang.

- *Mã nguồn:* Các mã nguồn phần mềm ứng dụng, website.

- *Sao lưu dữ liệu:* Là việc sao chép để lưu giữ dự phòng toàn bộ mã nguồn, dữ liệu lên một máy chủ lưu dự phòng.

- *Phục hồi dữ liệu*: Là khi hệ thống có sự cố và bị mất dữ liệu, có thể dùng dữ liệu dự phòng để thay thế, phục hồi lại dữ liệu trên hệ thống.

- *Sao lưu tự động:* Là tự động sao lưu lại tất cả những dữ liệu mới được phát sinh theo lịch đã được lập. Tất cả dữ liệu được sao lưu tự động qua các bước sau:

+ Xác định dữ liệu cần sao lưu.

+ Đặt lịch sao lưu tự động.

+ Khai báo địa chỉ lưu dữ liệu.

+ Kiểm tra thường xuyên dữ liệu được sao lưu, đảm bảo dữ liệu sao lưu phải được toàn vẹn.

- *Phân loại dữ liệu:* Cơ sở dữ liệu, dữ liệu kế toán, dữ liệu văn bản, bản tính,....

Các từ viết tắt

- CNTT: Công nghệ thông tin

- HĐH: Hệ điều hành Windows, Linux.

4. Nội dung quy trình

4.1. Quy trình quản lý an toàn máy chủ và ứng dụng

Bước 1: Quản lý máy chủ

Phân loại máy chủ theo chức năng:

- Máy chủ ứng dụng (website...)

- Máy chủ cơ sở dữ liệu (SQL, Oracle...)

- Máy chủ tệp (Tập tin Server, NAS)

- Máy chủ ảo hóa

Mỗi máy chủ phải được thống kê chi tiết các nội dung như sau:

- Cấu hình chi tiết (CPU, RAM, ổ cứng, hệ điều hành, IP, chức năng, người quản trị).

- Mã định danh duy nhất (VD: SVR-WEB-01).

- Cập nhật nhật ký hoạt động (log system, access log).

Tất cả truy cập quản trị máy chủ phải qua tài khoản quản trị được ủy quyền, có mật khẩu mạnh và thay đổi định kỳ 3 tháng/lần.

Bước 2: Xác định danh sách tài khoản và quyền truy cập

Chỉ Văn phòng HĐND - UBND, Văn phòng Đảng Ủy hoặc đơn vị được ủy quyền mới được phép cài đặt, cấu hình máy chủ.

Cấu hình hệ thống phải tuân thủ:

- Tắt hoặc gỡ bỏ dịch vụ, cổng (port) không cần thiết.

- Bật tường lửa nội bộ (Windows Firewall / iptables).

- Thiết lập quyền truy cập thư mục, chia sẻ, CSDL đúng mức cần thiết (Least Privilege).

- Cấu hình sau khi hoàn tất phải được lưu lại dạng tập tin và in biên bản nghiệm thu kỹ thuật.

Bước 3: Quản lý cập nhật và bản vá

Cập nhật hệ điều hành, ứng dụng và dịch vụ theo lịch:

- Hệ điều hành: kiểm tra và cập nhật hàng quý hoặc khi có bản vá quan trọng.
- Phần mềm ứng dụng: theo khuyến nghị của nhà cung cấp.
- Cơ sở dữ liệu: vá lỗi bảo mật định kỳ hoặc theo cảnh báo.

Trước khi áp dụng bản vá trên hệ thống thật, phải:

- Thử nghiệm trong môi trường mô phỏng.
- Có biên bản kiểm tra và phê duyệt.

Bước 4: Quản lý truy cập và phân quyền

Tài khoản truy cập máy chủ:

- Cấp phát theo danh sách đã phê duyệt .
- Không khuyến nghị sử dụng tài khoản dùng chung.
- Ghi lại toàn bộ nhật ký truy cập (access log, RDP log, SSH log).

Với ứng dụng:

- Phân quyền người dùng theo chức năng công việc (Chức vụ, phòng ban…).

Bước 5: Sao lưu và khôi phục

Văn phòng HĐND - UBND, Văn phòng Đảng Ủy thực hiện sao lưu:

- Dữ liệu hệ thống (CSDL ĐẢNG ỦY, HĐND, UBND xã Phước Giang).
- Cấu hình máy chủ, ứng dụng.
- Nhật ký truy cập và bảo mật.

Chính sách sao lưu:

- Sao lưu hàng ngày (tự động) và hàng tuần (offline).
- Lưu trữ ít nhất 02 bản (trên máy chủ, ổ cứng ngoài và đám mây hoặc băng từ).

Định kỳ thử khôi phục dữ liệu 03 tháng/lần để đảm bảo khả năng phục hồi sau sự cố.

Bước 6: Giám sát an toàn và cảnh báo

Lấy log (nhật ký) của thiết bị, ứng dụng để:

- Phát hiện truy cập trái phép, hành vi bất thường.
- Điều tra, truy vết, ứng cứng sự cố.

Lưu trữ log hệ thống ít nhất 12 tháng.

Phân tích log hàng tuần, báo cáo tóm tắt hàng quý hoặc khi có bất thường cho Lãnh đạo ĐẢNG ỦY, HĐND, UBND xã Phước Giang.

Bước 7: Quản lý ứng dụng

Tất cả phần mềm, ứng dụng phải được kiểm thử bảo mật (security test) trước khi triển khai.

Cấm cài đặt phần mềm không có bản quyền hoặc không rõ nguồn gốc.

Ứng dụng web khuyến cáo:

- Dùng HTTPS, chứng chỉ SSL hợp lệ.

- Kiểm tra và vá các lỗ hổng OWASP Top 10.

Các API hoặc tích hợp liên hệ với bên ngoài phải có cơ chế kiểm soát truy cập và mã hóa dữ liệu.

Bước 8: Xử lý sự cố và khôi phục sau sự cố

Khi phát hiện:

- Máy chủ bị tấn công, lỗi truy cập CSDL, dịch vụ ngừng hoạt động.

- Văn phòng HĐND – UBND phối hợp cán bộ phụ trách CNTT phải ngắt kết nối mạng, cô lập hệ thống, trích xuất log.

- Lập biên bản sự cố, báo cáo Lãnh đạo và cơ quan chuyên trách ATTT nếu nghiêm trọng.

Sau xử lý, phải:

- Kiểm tra lại toàn bộ tài khoản và nhật ký.

- Cập nhật bản vá, đổi mật khẩu quản trị.

- Rà soát nguyên nhân gốc (Root Cause Analysis).

Bước 9: Kiểm tra và đánh giá định kỳ

Thực hiện kiểm tra an toàn máy chủ và ứng dụng hàng quý, bao gồm:

- Quét lỗ hổng bảo mật.

- Đánh giá hiệu năng, tải và nhật ký truy cập.

- Kiểm tra quyền truy cập, tài khoản tồn đọng.

Báo cáo kết quả và kế hoạch khắc phục gửi Ban Lãnh đạo phê duyệt.

5. Hiệu lực thi hành

Quy trình có hiệu lực kể từ ngày ký ban hành.

Văn phòng HĐND - UBND, Văn phòng Đảng Ủy chịu trách nhiệm phổ biến, hướng dẫn thực hiện.

Hồ sơ, log và biểu mẫu được lưu giữ tối thiểu 05 năm.

QUY TRÌNH
QUẢN LÝ AN TOÀN DỮ LIỆU

Quảng Ngãi - năm 2026

ỦY BAN NHÂN DÂN XÃ PHƯỚC GIANG

QUY TRÌNH
Quản lý an toàn dữ liệu

	Người lập	Người xem xét	Người phê duyệt
Họ tên	Võ Thế Duy	Lê Viết Hiệp	Nguyễn Văn Lễ
Ký tên			
Chức vụ	Cán bộ phụ trách chuyển đổi số và ATTT - ANM	Chánh Văn phòng HĐND và UBND	Chủ tịch UBND
Ngày			

Số: 1653/QĐ-UBND Ngày ban hành: 14/8/2026

Quảng Ngãi - năm 2026

QUY TRÌNH
Quản lý an toàn dữ liệu

1. Mục đích

Thiết lập và duy trì quy trình bảo đảm an toàn cho toàn bộ dữ liệu hành chính, kỹ thuật của ĐẢNG ỦY, HĐND, UBND xã Phước Giang trong suốt vòng đời dữ liệu, bao gồm: thu thập, lưu trữ, sử dụng, chia sẻ, truyền tải, sao lưu và hủy bỏ, nhằm phòng ngừa mất mát, rò rỉ hoặc truy cập trái phép.

2. Phạm vị áp dụng

2.1 Đối tượng áp dụng

Áp dụng cho mọi loại dữ liệu được tạo ra, xử lý, hoặc lưu trữ bởi ĐẢNG ỦY, HĐND, UBND xã Phước Giang và các phòng ban, bao gồm:

Dữ liệu văn bản hành chính công vụ

Dự liệu bảng biểu, số liệu, thống kê

Dữ liệu quản trị (nhân sự, tài chính, kế hoạch, hồ sơ pháp lý).

Dữ liệu hệ thống CNTT (log, cấu hình, bản sao lưu, chứng thư số).

Áp dụng cho toàn thể cán bộ, nhân viên, đối tác, nhà cung cấp dịch vụ CNTT có liên quan đến dữ liệu của ĐẢNG ỦY, HĐND, UBND xã Phước Giang.

2.2 Trách nhiệm áp dụng

Đơn vị / Bộ phận	Trách nhiệm chính
Văn phòng HĐND - UBND, Văn phòng Đảng Ủy	Quản lý kỹ thuật, kiểm soát truy cập, mã hóa, sao lưu và phục hồi dữ liệu.
Các phòng ban	Quản lý dữ liệu nhân sự, hồ sơ lao động. Quản lý dữ liệu tài chính, báo cáo kế toán, chi phí bảo hiểm. Cập nhật, sử dụng dữ liệu đúng thẩm quyền; báo cáo sự cố khi có nghi ngờ rò rỉ.

3. Định nghĩa, từ viết tắt

3.1. Định nghĩa

**Admin*: Chánh Văn phòng HĐND - UBND, Văn phòng Đảng Ủy, người chịu trách nhiệm quản lý sự vận hành toàn bộ hệ thống mạng;

**Hệ thống CNTT*: Toàn bộ cơ sở hạ tầng trang thiết bị CNTT, hệ thống phần cứng, phần mềm, CSDL thiết lập nên hệ thống CNTT cũng như hệ thống logic CNTT của ĐẢNG ỦY, HĐND, UBND xã Phước Giang;

**Hệ thống Server:* Là hệ thống các máy chủ đặt tại phòng Sever, từ đây hệ thống máy chủ các thiết bị mạng, được kết nối với nhau để thiết lập nên mạng logic vận hành hoạt động ổn định thông suốt trong toàn ĐẢNG ỦY, HĐND, UBND xã Phước Giang.

Mã nguồn: Các mã nguồn phần mềm ứng dụng, website.

Sao lưu dữ liệu: Là việc sao chép để lưu giữ dự phòng toàn bộ mã nguồn, dữ liệu lên một máy chủ lưu dự phòng.

Phục hồi dữ liệu: Là khi hệ thống có sự cố và bị mất dữ liệu, có thể dùng dữ liệu dự phòng để thay thế, phục hồi lại dữ liệu trên hệ thống.

Sao lưu tự động: Là tự động sao lưu lại tất cả những dữ liệu mới được phát sinh theo lịch đã được lập. Tất cả dữ liệu được sao lưu tự động qua các bước sau:

+ Xác định dữ liệu cần sao lưu.

+ Đặt lịch sao lưu tự động.

+ Khai báo địa chỉ lưu dữ liệu.

+ Kiểm tra thường xuyên dữ liệu được sao lưu, đảm bảo dữ liệu sao lưu phải được toàn vẹn.

Phân loại dữ liệu: Cơ sở dữ liệu, dữ liệu kế toán, dữ liệu văn bản, bản tính,....

Các từ viết tắt

*CNTT: Công nghệ thông tin

* HĐH: Hệ điều hành Windows, Linux.

4. Nội dung quy trình

4.1. Quy trình quản lý an toàn dữ liệu

Bước 1: Phân loại dữ liệu

Tất cả dữ liệu của ĐẢNG ỦY, HĐND, UBND xã Phước Giang được phân loại theo mức độ nhạy cảm:

Mức độ	Loại dữ liệu	Biện pháp bảo vệ
Mức 1 – Mật	Văn bản bí mật Đảng, nhà nước,	Mã hóa AES-256, giới hạn truy cập theo cá nhân, chỉ được trao đổi trong Mạng thông tin bí mật.
Mức 2 – Nhạy cảm	Dữ liệu nhân sự, tài chính, hợp đồng, báo cáo chuyên môn	Mã hóa lưu trữ, truy cập theo vai trò, lưu log đầy đủ.
Mức 3 – Nội bộ	Văn bản điều hành, kế hoạch công tác	Bảo vệ bằng mật khẩu, chỉ truy cập nội bộ.
Mức 4 – Công khai	Thông tin tuyên truyền, thông cáo báo chí	Kiểm duyệt trước khi công bố.

Phân loại dữ liệu được thực hiện và cập nhật **hàng năm** hoặc khi có thay đổi hệ thống.

Bước 2: Thu thập và tạo lập dữ liệu

Chỉ thu thập dữ liệu cần thiết cho mục đích nghiệp vụ.

Dữ liệu khi nhập vào hệ thống phải được kiểm tra tính chính xác và toàn vẹn (checksum, mã xác thực).

Bước 3: Lưu trữ và bảo quản dữ liệu

Tất cả dữ liệu không mật được lưu trữ trên:

Máy tính cá nhân của cán bộ, công chức, viên chức, người lao đồng.

Văn thư lưu trữ văn bản giấy hoặc tập tin dữ liệu.

Văn phòng HĐND - UBND, Văn phòng Đảng Ủy thực hiện:

Mã hóa toàn bộ ổ đĩa lưu trữ dữ liệu khi cần thiết.

Giới hạn quyền truy cập thư mục theo nhóm người dùng.

Thiết lập hệ thống kiểm soát truy cập (Access Control) và ghi log đầy đủ.

Dữ liệu giấy phải:

Lưu tại phòng lưu trữ chuyên dụng, có khóa và camera giám sát.

Thời hạn lưu theo quy định.

Bước 4: Sử dụng và chia sẻ dữ liệu

Dữ liệu chỉ được truy cập hoặc chia sẻ khi có thẩm quyền phê duyệt.

Khi chia sẻ dữ liệu:

Phải ẩn danh (de-identification) thông tin cá nhân nếu phục vụ nghiên cứu, thống kê.

Dùng kênh bảo mật (VPN, HTTPS, SFTP) nếu cần thiết.

Ghi lại nhật ký chia sẻ (người gửi, người nhận, nội dung, thời điểm).

Cấm sao chép dữ liệu được bảo vệ ra các thiết bị cá nhân (USB, laptop) nếu chưa được phép bằng văn bản.

Bước 5: Bảo vệ và mã hóa dữ liệu

Áp dụng mã hóa AES-256 hoặc tương đương đối với:

Dữ liệu quan trọng.

Dữ liệu truyền tải qua mạng (SSL/TLS).

Bật tự động khóa màn hình sau 5 phút không hoạt động.

Không lưu mật khẩu hoặc dữ liệu nhạy cảm trong tập tin văn bản, email hoặc ứng dụng chat.

Bước 6: Sao lưu và khôi phục dữ liệu

Văn phòng HĐND - UBND, Văn phòng Đảng Ủy thiết lập kế hoạch sao lưu đối với các dữ liệu quan trọng như sau:

Hằng ngày: sao lưu dữ liệu nghiệp vụ.

Hằng tuần: sao lưu toàn bộ hệ thống.

Hằng tháng: lưu trữ bản sao ra thiết bị offline.

Kiểm tra tính toàn vẹn bản sao lưu 1 lần/tháng và diễn tập khôi phục dữ liệu 03 tháng/lần.

Bản sao lưu được lưu tối thiểu 90 ngày, lưu ít nhất 02 bản trên các thiết bị khác nhau.

Bước 7: Hủy bỏ dữ liệu

Dữ liệu hết hạn hoặc không còn sử dụng phải được hủy an toàn và có kiểm soát:

Dữ liệu điện tử: xóa vĩnh viễn, ghi đè bằng công cụ chuyên dụng.

Dữ liệu giấy: hủy bằng máy cắt hoặc thiêu hủy có biên bản.

Việc hủy dữ liệu phải có biên bản và phê duyệt của Ban Lãnh đạo.

Bước 8: Giám sát và phát hiện sự cố dữ liệu

Văn phòng HĐND - UBND, Văn phòng Đảng Ủy thiết lập hệ thống giám sát truy cập dữ liệu (Data Access Monitoring) nếu có.

Cảnh báo khi:

Có hành vi truy cập bất thường hoặc tải lượng dữ liệu lớn.

Có truy cập ngoài giờ hành chính hoặc từ IP lạ.

Khi phát hiện rò rỉ, phải kích hoạt quy trình quản lý sự cố an toàn thông tin

Bước 9: Đánh giá và rà soát định kỳ

Kiểm tra định kỳ hàng quý các nội dung:

Phân quyền truy cập, tài khoản còn hiệu lực.

Hiệu quả mã hóa, sao lưu và phục hồi.

Rủi ro rò rỉ và tuân thủ chính sách bảo mật.

Kết quả rà soát phải được lập thành báo cáo đánh giá An toàn dữ liệu và gửi Ban Lãnh đạo.

5. Hiệu lực thi hành

Quy trình có hiệu lực kể từ ngày ký.

Văn phòng HĐND - UBND, Văn phòng Đảng Ủy chịu trách nhiệm phổ biến, hướng dẫn, và kiểm tra việc tuân thủ.

Tài liệu, biểu mẫu, và nhật ký thực hiện được lưu giữ tối thiểu 10 năm.

QUY TRÌNH
QUẢN LÝ SỰ CỐ AN TOÀN THÔNG TIN

Quảng Ngãi - năm 2026

ỦY BAN NHÂN DÂN XÃ PHƯỚC GIANG

QUY TRÌNH
Quản lý sự cố an toàn thông tin

	Người lập	Người xem xét	Người phê duyệt
Họ tên	Võ Thế Duy	Lê Viết Hiệp	Nguyễn Văn Lễ
Ký tên			
Chức vụ	Cán bộ phụ trách chuyển đổi số và ATTT - ANM	Chánh Văn phòng HĐND và UBND	Chủ tịch UBND
Ngày			

Số: 1653/QĐ-UBND Ngày ban hành: 14/8/2026

Quảng Ngãi - năm 2026

QUY TRÌNH
Quản lý sự cố an toàn thông tin

1. Mục đích

Thiết lập quy trình chuẩn để phát hiện, ghi nhận, xử lý, khắc phục và báo cáo các sự cố an toàn thông tin (ATTT), nhằm giảm thiểu thiệt hại, đảm bảo hoạt động liên tục của hệ thống thông tin, và ngăn ngừa tái diễn.

2. Phạm vị áp dụng

2.1 Đối tượng áp dụng

Áp dụng cho toàn bộ hệ thống thông tin, máy chủ, thiết bị mạng, cơ sở dữ liệu, ứng dụng và dịch vụ CNTT của ĐẢNG ỦY, HĐND, UBND xã Phước Giang .

Áp dụng cho mọi cán bộ, nhân viên, kỹ thuật viên CNTT, đơn vị vận hành hoặc nhà cung cấp có liên quan đến quản trị, sử dụng hoặc khai thác dữ liệu và hệ thống CNTT của ĐẢNG ỦY, HĐND, UBND xã Phước Giang.

2.2 Trách nhiệm áp dụng

Đơn vị / Bộ phận	Trách nhiệm chính
Người sử dụng hệ thống	Phát hiện và báo cáo ngay sự cố hoặc hành vi nghi ngờ rò rỉ, tấn công, xâm nhập.
Văn phòng HĐND - UBND, Văn phòng Đảng Ủy	Tiếp nhận, đánh giá, phân loại, cô lập, xử lý và khôi phục hệ thống; lưu trữ nhật ký và báo cáo.
Đơn vị chuyên trách An toàn thông tin của Tỉnh	Phối hợp điều tra, phân tích nguyên nhân, khắc phục và lập báo cáo tổng hợp.
Ban Lãnh đạo	Phê duyệt biện pháp khắc phục, chỉ đạo ứng cứu khẩn cấp và báo cáo cơ quan chức năng khi cần.

3. Định nghĩa, từ viết tắt

Định nghĩa

- *Admin*: Chánh Văn phòng HĐND - UBND, Văn phòng Đảng Ủy, người chịu trách nhiệm quản lý sự vận hành toàn bộ hệ thống mạng;

- *Hệ thống CNTT*: Toàn bộ cơ sở hạ tầng trang thiết bị CNTT, hệ thống phần cứng, phần mềm, CSDL thiết lập nên hệ thống CNTT cũng như hệ thống logic CNTT của ĐẢNG ỦY, HĐND, UBND xã Phước Giang;

- *Hệ thống Server:* Là hệ thống các máy chủ đặt tại phòng Sever, từ đây hệ thống máy chủ các thiết bị mạng, được kết nối với nhau để thiết lập nên mạng logic vận hành hoạt động ổn định thông suốt trong toàn ĐẢNG ỦY, HĐND, UBND xã Phước Giang.

- *Mã nguồn:* Các mã nguồn phần mềm ứng dụng, website.

- *Sao lưu dữ liệu:* Là việc sao chép để lưu giữ dự phòng toàn bộ mã nguồn, dữ liệu lên một máy chủ lưu dự phòng.

- *Phục hồi dữ liệu*: Là khi hệ thống có sự cố và bị mất dữ liệu, có thể dùng dữ liệu dự phòng để thay thế, phục hồi lại dữ liệu trên hệ thống.

- *Sao lưu tự động:* Là tự động sao lưu lại tất cả những dữ liệu mới được phát sinh theo lịch đã được lập. Tất cả dữ liệu được sao lưu tự động qua các bước sau:

+ Xác định dữ liệu cần sao lưu.

+ Đặt lịch sao lưu tự động.

+ Khai báo địa chỉ lưu dữ liệu.

+ Kiểm tra thường xuyên dữ liệu được sao lưu, đảm bảo dữ liệu sao lưu phải được toàn vẹn.

- *Phân loại dữ liệu:* Cơ sở dữ liệu, dữ liệu kế toán, dữ liệu văn bản, bản tính,....

Các từ viết tắt

- CNTT: Công nghệ thông tin

- HĐH: Hệ điều hành Windows, Linux.

4. Nội dung quy trình

4.1. Quy trình sao lưu

Bước 1: Phát hiện và ghi nhận sự cố

Sự cố ATTT bao gồm:

- Truy cập trái phép, tấn công mạng, mã độc, ransomware.

- Mất hoặc rò rỉ dữ liệu, xóa nhầm hoặc phá hoại dữ liệu.

- Lỗi hệ thống khiến gián đoạn hoạt động CNTT hoặc mất tính toàn vẹn dữ liệu.

- Thiết bị bị đánh cắp, mất cắp hoặc hư hỏng do lỗi bảo mật.

Các kênh phát hiện:

- Hệ thống giám sát (IDS/IPS, log server, firewall, antivirus).

- Báo cáo thủ công từ người dùng.

- Cảnh báo từ đối tác, cơ quan chuyên trách (VD: PA05, VNCERT, VNISA).

Mọi sự cố phải được ghi nhận vào Sổ theo dõi sự cố ATTT, bao gồm: thời gian, người phát hiện, mô tả sơ bộ, ảnh hưởng ban đầu.

Bước 2: Thông báo và kích hoạt ứng cứu

Khi phát hiện sự cố, người dùng hoặc cán bộ kỹ thuật phải thông báo ngay cho Văn phòng HĐND - UBND, Văn phòng Đảng Ủy (qua điện thoại).

Trường hợp nghiêm trọng (ransomware, rò rỉ dữ liệu người dân, mất quyền truy cập hệ thống nội bộ…), Văn phòng HĐND - UBND, Văn phòng Đảng Ủy phải báo cáo khẩn cấp Lãnh đạo ĐẢNG ỦY, HĐND, UBND xã Phước Giang để kích hoạt Đội Ứng cứu sự cố (CERT) gồm:

- Trưởng Phòng ban trực tiếp sử dụng phối hợp cán bộ được phân công CNTT (Tổ trưởng).

- Đại diện lãnh đạo ĐẢNG ỦY, HĐND, UBND xã Phước Giang.

- Đơn vị phụ trách An toàn thông tin trên địa bàn tỉnh.

- Đại diện đơn vị bị ảnh hưởng.

Bước 3: Phân loại và đánh giá mức độ sự cố

Mức độ	Tiêu chí	Ví dụ
Mức 1 – Nhẹ	Không ảnh hưởng hoạt động, dễ khắc phục	Lỗi tài khoản, máy trạm nhiễm virus đơn lẻ
Mức 2 – Trung bình	Ảnh hưởng cục bộ, có thể khôi phục trong 24h	Hệ thống nội bộ, lỗi cấu hình máy chủ phụ
Mức 3 – Nghiêm trọng	Ảnh hưởng toàn hệ thống hoặc dữ liệu nhạy cảm bị rò rỉ	Mất CSDL nội bộ, tấn công ransomware, rò rỉ hồ sơ
Mức 4 – Đặc biệt nghiêm trọng	Ảnh hưởng toàn ĐẢNG ỦY, HĐND, UBND xã Phước Giang hoặc vi phạm pháp luật về ATTT	Tấn công phá hoại, đánh cắp dữ liệu quy mô lớn

Bước 4: Cô lập và kiểm soát sự cố

Khi sự cố xảy ra, phải cô lập ngay hệ thống bị ảnh hưởng, ví dụ:

- Ngắt kết nối mạng hoặc Internet.
- Dừng dịch vụ hoặc máy chủ liên quan.
- Ngăn chặn lan truyền mã độc.
- Không xóa hoặc ghi đè log, dữ liệu để đảm bảo phục vụ điều tra.

Lưu lại ảnh chụp màn hình, bản sao log, thời gian xảy ra, tài khoản liên quan.

Bước 5: Phân tích, điều tra nguyên nhân

Đội CERT thu thập thông tin:

- Log hệ thống (Firewall, Server, Database, Endpoint).
- Tập tin nghi ngờ, mẫu mã độc (nếu có).
- Các thao tác người dùng trước thời điểm sự cố.

Xác định nguyên nhân gốc (Root Cause Analysis):

- Lỗi con người (misconfiguration, lộ mật khẩu).
- Lỗi phần mềm hoặc phần cứng.
- Tấn công mạng từ bên ngoài.

Đề xuất biện pháp xử lý và khắc phục phù hợp.

Bước 6: Xử lý và khôi phục hệ thống

Tiến hành khôi phục hệ thống theo các bước:

- Diệt mã độc, vá lỗi, thay đổi mật khẩu, phục hồi dữ liệu từ bản sao lưu.
- Kiểm tra tính toàn vẹn và hoạt động bình thường của hệ thống sau khôi phục.
- Ghi nhận lại toàn bộ quá trình xử lý trong Biên bản ứng cứu sự cố.

- Thông báo kết quả khôi phục cho các phòng ban liên quan.

Bước 7: Báo cáo người quản lý

Báo cáo sự cố bao gồm:

- Thông tin tóm tắt sự cố, thời điểm, hệ thống ảnh hưởng.

- Nguyên nhân, biện pháp xử lý, thiệt hại, thời gian phục hồi.

- Đề xuất biện pháp phòng ngừa tái diễn.

Báo cáo được lập bởi Văn phòng HĐND - UBND, Văn phòng Đảng Ủy và trình Lãnh đạo ĐẢNG ỦY, HĐND, UBND xã Phước Giang phê duyệt.

Với sự cố nghiêm trọng (mức 3, 4), phải:

- Báo cáo Công an tỉnh (qua Thường trực Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao tỉnh Quảng Ngãi) trong vòng 12 giờ kể từ khi phát hiện.

- Phối hợp Phối hợp với cơ quan chuyên trách nếu có yêu cầu điều tra.

Bước 8: Báo cáo người quản lý

Sau khi xử lý xong, Đội CERT tổ chức họp đánh giá sau sự cố (Post-Incident Review):

- Phân tích nguyên nhân gốc, điểm yếu trong quy trình hoặc kỹ thuật.

- Cập nhật chính sách bảo mật, vá lỗi hệ thống, tăng cường giám sát.

- Hướng dẫn lại nhân viên nếu sự cố do thao tác sai hoặc vi phạm quy định.

Ghi lại biên bản rút kinh nghiệm và cập nhật Kế hoạch phòng ngừa sự cố ATTT.

Bước 9: Lưu trữ hồ sơ và theo dõi

Hồ sơ sự cố gồm: báo cáo, log, biên bản ứng cứu, kết quả điều tra, rút kinh nghiệm.

Phòng ban trực tiếp sử dụng phối hợp cán bộ được phân công CNTT lưu giữ hồ sơ tối thiểu 05 năm, có thể kéo dài nếu sự cố liên quan pháp lý.

Các sự cố được tổng hợp định kỳ hàng quý để báo cáo cho Ban Lãnh đạo và phục vụ kiểm tra nội bộ.

5. Hiệu lực thi hành

Quy trình có hiệu lực kể từ ngày ký ban hành.

Văn phòng HĐND - UBND, Văn phòng Đảng Ủy chịu trách nhiệm phổ biến, hướng dẫn cán bộ và kiểm tra tuân thủ.

Hồ sơ, nhật ký sự cố được lưu giữ tối thiểu 05 năm để phục vụ công tác kiểm tra và đánh giá định kỳ.

QUY TRÌNH
QUẢN LÝ AN TOÀN NGƯỜI SỬ DỤNG ĐẦU CUỐI

Quảng Ngãi - năm 2025

ỦY BAN NHÂN DÂN XÃ PHƯỚC GIANG

QUY TRÌNH
Quản lý an toàn người sử dụng đầu cuối

	Người lập	Người xem xét	Người phê duyệt
Họ tên	Võ Thế Duy	Lê Viết Hiệp	Nguyễn Văn Lễ
Ký tên			
Chức vụ	Cán bộ phụ trách chuyển đổi số và ATTT - ANM	Chánh Văn phòng HĐND và UBND	Chủ tịch UBND
Ngày			

Số: 1653/QĐ-UBND Ngày ban hành: 14/8/2026

Quảng Ngãi - năm 2026

QUY TRÌNH
Quản lý an toàn người sử dụng đầu cuối

1. Mục đích

Thiết lập quy trình nhằm đảm bảo an toàn, bảo mật và tuân thủ trong việc sử dụng các thiết bị đầu cuối và tài nguyên CNTT bởi người dùng (cán bộ, nhân viên, đối tác), nhằm:

- Ngăn chặn truy cập trái phép, rò rỉ dữ liệu hoặc lây nhiễm mã độc từ thiết bị đầu cuối.

- Giảm thiểu rủi ro an ninh mạng xuất phát từ hành vi người dùng.

- Tăng cường nhận thức và trách nhiệm về an toàn thông tin trong toàn ĐẢNG ỦY, HĐND, UBND xã Phước Giang.

2. Phạm vị áp dụng

2.1 Đối tượng áp dụng

Áp dụng cho tất cả người sử dụng hệ thống thông tin, máy tính, thiết bị có kết nối mạng, thiết bị lưu trữ, và thiết bị di động thuộc sở hữu hoặc sử dụng .

Bao gồm cán bộ, nhân viên, sinh viên thực tập, đối tác, nhà cung cấp khi được cấp quyền truy cập hệ thống của ĐẢNG ỦY, HĐND, UBND xã Phước Giang.

2.2 Trách nhiệm áp dụng

Đơn vị / Bộ phận	Trách nhiệm chính
Văn phòng HĐND - UBND, Văn phòng Đảng Ủy	Quản lý kỹ thuật, cấp phát và thu hồi tài khoản, triển khai phần mềm bảo mật, giám sát hành vi người dùng.
Người sử dụng đầu cuối	Tuân thủ quy định ATTT, bảo vệ thiết bị cá nhân, mật khẩu và dữ liệu được giao.
Trưởng Các phòng ban	Giám sát nhân viên thuộc đơn vị trong việc chấp hành quy định ATTT.
Ban Lãnh đạo	Phê duyệt chính sách, xử lý vi phạm và tổ chức đào tạo định kỳ.

3. Định nghĩa, từ viết tắt

3.1. Định nghĩa

- *Admin*: Chánh Văn phòng HĐND - UBND, Văn phòng Đảng Ủy, người chịu trách nhiệm quản lý sự vận hành toàn bộ hệ thống mạng;

- *Hệ thống CNTT*: Toàn bộ cơ sở hạ tầng trang thiết bị CNTT, hệ thống phần cứng, phần mềm, CSDL thiết lập nên hệ thống CNTT cũng như hệ thống logic CNTT của ĐẢNG ỦY, HĐND, UBND xã Phước Giang;

- *Hệ thống Server:* Là hệ thống các máy chủ đặt tại phòng Sever, từ đây hệ thống máy chủ các thiết bị mạng, được kết nối với nhau để thiết lập nên mạng logic vận hành hoạt động ổn định thông suốt trong toàn ĐẢNG ỦY, HĐND, UBND xã Phước Giang.

- *Mã nguồn:* Các mã nguồn phần mềm ứng dụng, website.

- *Sao lưu dữ liệu:* Là việc sao chép để lưu giữ dự phòng toàn bộ mã nguồn, dữ liệu lên một máy chủ lưu dự phòng.

- *Phục hồi dữ liệu*: Là khi hệ thống có sự cố và bị mất dữ liệu, có thể dùng dữ liệu dự phòng để thay thế, phục hồi lại dữ liệu trên hệ thống.

- *Sao lưu tự động:* Là tự động sao lưu lại tất cả những dữ liệu mới được phát sinh theo lịch đã được lập. Tất cả dữ liệu được sao lưu tự động qua các bước sau:

+ Xác định dữ liệu cần sao lưu.

+ Đặt lịch sao lưu tự động.

+ Khai báo địa chỉ lưu dữ liệu.

+ Kiểm tra thường xuyên dữ liệu được sao lưu, đảm bảo dữ liệu sao lưu phải được toàn vẹn.

- *Phân loại dữ liệu:* Cơ sở dữ liệu, dữ liệu kế toán, dữ liệu văn bản, bản tính,....

Các từ viết tắt

- CNTT: Công nghệ thông tin

- HĐH: Hệ điều hành Windows, Linux.

4. Nội dung quy trình

4.1. Quy trình sao lưu

Bước 1: Cấp quyền và khởi tạo người dùng

- Mỗi người dùng được cấp một tài khoản duy nhất, không dùng chung.

- Quyền truy cập được cấp theo chức năng công việc và nguyên tắc "ít quyền nhất" (Least Privilege).

- Tài khoản chỉ có hiệu lực trong thời gian làm việc; khi nhân sự nghỉ, chuyển công tác hoặc tạm nghỉ, Phòng ban trực tiếp sử dụng phối hợp cán bộ được phân công CNTT phải vô hiệu hóa ngay tài khoản.

- Tài khoản quản trị (admin) chỉ cấp cho nhân viên CNTT được ủy quyền, có biên bản phê duyệt.

Bước 2: Xác định danh sách tài khoản và quyền truy cập

Người dùng phải:

- Đăng nhập bằng tài khoản cá nhân.

- Không chia sẻ, tiết lộ hoặc lưu mật khẩu ở dạng rõ ràng (plain text).

- Sử dụng mật khẩu mạnh (≥ 8 ký tự, có chữ hoa, số, ký tự đặc biệt), đổi ít nhất 3 tháng/lần.

- Khóa màn hình khi rời máy (≤ 5 phút).

Không tự ý:

- Cài đặt phần mềm không rõ nguồn gốc.

- Kết nối thiết bị ngoại vi như: USB, điện thoại hoặc ổ cứng ngoài nếu chưa được phép.

- Sử dụng tài khoản cá nhân (Facebook, Gmail...) để lưu trữ dữ liệu công việc.

Thiết bị đầu cuối phải:

- Cài đặt phần mềm antivirus, firewall và công cụ quản lý do Phòng ban trực tiếp sử dụng phối hợp cán bộ được phân công CNTT triển khai.

- Cập nhật bản vá hệ điều hành và phần mềm

Bước 3: Sử dụng email, Internet và phần mềm trực tuyến

- Chỉ sử dụng email công vụ cho công việc.

- Không mở tập tin đính kèm, liên kết (link) hoặc email từ nguồn không tin cậy.

- Không tải phần mềm hoặc tài liệu từ website không rõ nguồn gốc.

- Không đăng tải thông tin người khác, tài liệu nội bộ hoặc dữ liệu chuyên môn lên mạng xã hội, diễn đàn, hoặc nền tảng chia sẻ công khai.

Bước 4: Bảo vệ dữ liệu người dùng

Người dùng có trách nhiệm bảo vệ dữ liệu mình tạo hoặc xử lý:

- Lưu trữ trên thư mục được phân quyền của hệ thống (server nội bộ).

- Không lưu dữ liệu người dân trên thiết bị cá nhân.

- Không sao chép dữ liệu ra thiết bị ngoài nếu không có sự đồng ý của Lãnh đạo và Phòng ban trực tiếp sử dụng phối hợp cán bộ được phân công CNTT.

Mọi sao lưu, chia sẻ hoặc truyền tải dữ liệu phải qua kênh bảo mật (VPN, SFTP, HTTPS) nếu có.

Bước 5: Phát hiện và báo cáo sự cố

Khi phát hiện các dấu hiệu sau, người dùng phải báo ngay cho Văn phòng HĐND - UBND, Văn phòng Đảng Ủy:

- Máy tính hoạt động bất thường (treo, tự khởi động, mất dữ liệu).

- Thông báo lỗi bảo mật, virus, hoặc truy cập lạ.

- Email đáng ngờ, hoặc nghi ngờ bị lộ mật khẩu.

Văn phòng HĐND - UBND, Văn phòng Đảng Ủy sau khi nhận được thong báo, thực hiện:

- Cô lập thiết bị, phân tích log, xử lý mã độc.

- Lập Biên bản sự cố người dùng đầu cuối.

- Báo cáo Ban Lãnh đạo nếu sự cố nghiêm trọng (rò rỉ dữ liệu, mất tài khoản).

Bước 6: Kiểm tra và giám sát người dùng

Phòng ban trực tiếp sử dụng phối hợp cán bộ được phân công CNTT thiết lập hệ thống:

- Ghi nhật ký truy cập (log login/logout, IP, hành vi truy cập dữ liệu).

- Giám sát thiết bị đầu cuối bằng phần mềm quản lý tập trung (Endpoint Management).

Định kỳ 3 tháng/lần, thực hiện:

- Rà soát danh sách tài khoản, quyền truy cập.

- Phát hiện tài khoản không sử dụng, tài khoản nghi ngờ.

- Báo cáo kết quả kiểm tra cho Lãnh đạo.

Bước 7: Đào tạo và nâng cao nhận thức

Tổ chức tập huấn định kỳ hàng năm về:

- Nhận diện email giả mạo, phishing.

- Cách bảo vệ dữ liệu cá nhân và mật khẩu.

- Ứng xử an toàn trên mạng.

Các nhân viên mới phải được đào tạo an toàn thông tin cơ bản trước khi được cấp tài khoản truy cập.

Bước 8: Xử lý vi phạm

Người sử dụng đầu cuối vi phạm quy định an toàn thông tin có thể bị:

- Cảnh cáo, tạm ngưng tài khoản, hoặc kỷ luật tùy mức độ.

- Bồi thường thiệt hại nếu gây hậu quả nghiêm trọng (rò rỉ dữ liệu người dân, phá hoại hệ thống).

Văn phòng HĐND - UBND, Văn phòng Đảng Ủy ghi nhận và lưu hồ sơ xử lý.

5. Hiệu lực thi hành

Quy trình có hiệu lực kể từ ngày ký ban hành.

Văn phòng HĐND - UBND, Văn phòng Đảng Ủy chịu trách nhiệm hướng dẫn, giám sát và đánh giá việc thực hiện.

Hồ sơ, biên bản và nhật ký liên quan được lưu giữ tối thiểu 05 năm.