ỦY BAN NHÂN DÂN **XÃ THANH ĐỊNH**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 292 /UBND-VP V/v đảm bảo an toàn thông tin trên Hệ thống thông tin giải quyết thủ tục hành chính tỉnh Thái Nguyên	*Thanh Định, ngày 10 tháng 10 năm 2024*

Kính gửi: Các Bộ phận chuyên môn thuộc UBND xã

Thực hiện Công văn số 6308/UBND-VP ngày 07/10/2024 của UBND huyện Định Hoá về việc đảm bảo an toàn thông tin trên Hệ thống thông tin giải quyết thủ tục hành chính tỉnh Thái Nguyên; UBND xã đề nghị các Bộ phận chuyên môn thuộc UBND xã triển khai thực hiện các nhiệm vụ sau:

1. Các Bộ phận chuyên môn, Bộ phận Tiếp nhận và Trả kết quả xã được cấp tài khoản thuộc phạm vi quản lý, nâng cao nhận thức, trách nhiệm, chấp hành nghiêm quy định về đảm bảo an toàn thông tin tài khoản cá nhân khi tham gia vào các hệ thống thông tin dùng chung theo quy định tại khoản 1, Điều 6 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước trên địa bàn tỉnh Thái Nguyên ban hành kèm theo Quyết định số 10/2020/QĐ-UBND ngày 08/5/2020 của UBND tỉnh Thái Nguyên[1].

2. Ngày 09/10/2024 (Thứ tư), Sở Thông tin và Truyền thực hiện nâng cấp chức năng đăng nhập trên Hệ thống thông tin giải quyết thủ tục hành chính. Vì vậy, Các Bộ phận chuyên môn, Bộ phận Tiếp nhận và Trả kết quả xã được cấp tài khoản tiếp nhận và xử lý hồ sơ thủ tục hành chính trên Hệ thống thông tin giải quyết thủ tục hành chính tỉnh Thái Nguyên thực hiện thay đổi mật khẩu đảm bảo theo điểm đ, khoản 1, Điều 6 Quyết định số 10/2020/QĐ-UBND ngày 08/5/2020 của UBND tỉnh Thái Nguyên.

UBND xã đề nghị Các Bộ phận chuyên môn, Bộ phận Tiếp nhận và Trả kết quả xã nghiêm túc triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Lãnh đạo UBND;
- Lưu: VP.

CHỦ TỊCH

Phùng Văn Đăng

---

[1] **Điều 6. Quản lý truy cập**
1. Đối với Cơ quan, đơn vị, người sử dụng có trách nhiệm
a) Bảo vệ bí mật thông tin tài khoản cá nhân, hoặc tài khoản của cơ quan, đơn vị khi được phân công nắm giữ đồng thời phải thay đổi ngay mật khẩu tài khoản khi mới được cấp và tự chịu trách nhiệm trong việc quản lý, bảo vệ mật khẩu của tài khoản, không được cho người khác sử dụng tài khoản cá nhân hoặc của cơ quan, đơn vị;
b) Không đặt chế độ tự động ghi nhớ mật khẩu của các trình duyệt trong mọi trường hợp sử dụng;
c) Thiết lập mật mã truy cập và chế độ tự động bảo vệ màn hình sau 10 phút không sử dụng cho tất cả hệ thống máy chủ, máy trạm của người sử dụng;
d) Hệ thống mạng không dây (wifi) của các cơ quan, đơn vị phải được đặt mật khẩu (password) khi truy cập. Thiết lập phương pháp hạn chế người dùng truy cập mạng không dây, giám sát và điều khiển truy cập mạng không dây;
đ) Đặt mật khẩu đăng nhập, truy cập hệ thống thông tin có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như !, @, #, $, %) và phải được thay đổi ít nhất 03 tháng/lần cho tất cả các tài khoản truy cập vào hệ thống máy chủ, thiết bị mạng, máy tính, các ứng dụng;
e) Các cơ quan, đơn vị cần rà soát tối thiểu 03 tháng/lần các tài khoản đăng nhập, bảo đảm các tài khoản và quyền truy cập hệ thống được cấp phát đúng, đủ.