UBND TỈNH ĐỒNG NAI **SỞ NỘI VỤ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 01010 /QĐ-SNV	*Đồng Nai, ngày 04 tháng 10 năm 2025*

QUYẾT ĐỊNH

Ban hành Quy chế sử dụng máy tính Client, máy chủ (Server) và hệ thống mạng nội bộ nhằm đảm bảo an toàn thông tin tại Sở Nội vụ tỉnh Đồng Nai

GIÁM ĐỐC SỞ NỘI VỤ

Căn cứ Luật Công nghệ thông tin 2006;

Căn cứ Luật An toàn thông tin mạng năm 2015;

Căn cứ Luật An ninh mạng 2018;

Căn cứ Nghị định số 147/2024/QĐ-CP ngày 09/11/2024 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng;

Căn cứ Quyết định số 05/2025/QĐ-UBND ngày 01 tháng 7 năm 2025 của Ủy ban nhân dân tỉnh Đồng Nai về việc ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Nội vụ;

Theo đề nghị của Chánh Văn phòng Sở Nội vụ tỉnh Đồng Nai.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy chế sử dụng máy tính Client, máy chủ (Server) và hệ thống mạng nội bộ nhằm đảm bảo an toàn thông tin tại Sở Nội vụ tỉnh Đồng Nai"**.**

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

Điều 3. Chánh Văn phòng Sở, Trưởng các Phòng chuyên môn, đơn vị thuộc Sở và toàn thể công chức, viên chức, người lao động thuộc Sở chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Giám đốc, các Phó Giám đốc;
- Trưởng PCM, ĐVTT;
- Lưu: VT, VP.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ NỘI VỤ
TỈNH ĐỒNG NAI

Nguyễn Hữu Định

UBND TỈNH ĐỒNG NAI
SỞ NỘI VỤ

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

QUY CHẾ
Về việc quản lý, sử dụng và bảo đảm an toàn thông tin trên hệ thống máy tính, máy chủ và mạng máy tính của Sở Nội vụ

(Ban hành kèm theo Quyết định số: 1010/QĐ-SNV ngày 04/ 10/2025 của Giám đốc Sở Nội vụ)

CHƯƠNG I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. **Phạm vi điều chỉnh:** Quy chế này quy định về việc quản lý, khai thác, sử dụng và các biện pháp bảo đảm an toàn thông tin trên hệ thống máy tính, máy chủ, hạ tầng mạng và các phần mềm ứng dụng (sau đây gọi chung là hệ thống CNTT) tại Sở Nội vụ tỉnh Đồng Nai.
2. **Đối tượng áp dụng:** Quy chế này áp dụng đối với tất cả công chức, viên chức và người lao động (sau đây gọi chung là người dùng) đang công tác tại Sở Nội vụ.

Điều 2. Mục đích, yêu cầu

1. **Mục đích:**

a) Nâng cao nhận thức, trách nhiệm của người dùng trong việc bảo vệ tài sản thông tin, dữ liệu của cơ quan.

b) Chuẩn hóa các quy trình quản lý, vận hành, sử dụng hệ thống CNTT, đảm bảo an toàn, an ninh thông tin, phòng chống các nguy cơ tấn công mạng.

c) Đảm bảo tính Bí mật, Toàn vẹn và Sẵn sàng của dữ liệu và hệ thống thông tin, phục vụ hiệu quả công tác chỉ đạo, điều hành và chuyên môn, nghiệp vụ của Sở.

d) Là cơ sở để xem xét, xử lý trách nhiệm đối với các cá nhân, tập thể có hành vi vi phạm.

2. **Yêu cầu:**

a) Mọi hoạt động quản lý, sử dụng hệ thống CNTT của Sở Nội vụ phải tuân thủ nghiêm ngặt các quy định tại Quy chế này và các quy định pháp luật có liên quan về an toàn thông tin, an ninh mạng.

b) Văn phòng Sở (bộ phận phụ trách CNTT) là đơn vị đầu mối, chịu trách nhiệm tham mưu, tổ chức triển khai, hướng dẫn và giám sát việc thực hiện Quy chế này.

Điều 3. Giải thích từ ngữ

Trong Quy chế này, các từ ngữ dưới đây được hiểu như sau:

1. *Hệ thống CNTT:* bao gồm hạ tầng kỹ thuật (máy chủ, máy trạm, thiết bị mạng, thiết bị lưu trữ, thiết bị an ninh...) và các phần mềm (hệ điều hành, phần mềm hệ thống, phần mềm ứng dụng dùng chung và chuyên ngành).
2. *Tài khoản người dùng (Account):* là thông tin định danh duy nhất cấp cho mỗi người dùng để truy cập vào hệ thống CNTT, bao gồm tên đăng nhập và mật khẩu.
3. *An toàn thông tin:* là việc bảo vệ thông tin, hệ thống thông tin tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép.

CHƯƠNG II
TRÁCH NHIỆM CỦA CÁC ĐƠN VỊ, CÁ NHÂN

Điều 4. Trách nhiệm của Văn phòng Sở (Bộ phận phụ trách CNTT)

1. Quản trị, vận hành, duy trì hoạt động ổn định và an toàn cho toàn bộ hệ thống CNTT của Sở.
2. Xây dựng và triển khai các giải pháp kỹ thuật nhằm đảm bảo an toàn thông tin: tường lửa, phần mềm diệt virus, hệ thống sao lưu dữ liệu, giám sát mạng.
3. Cấp phát, quản lý, thu hồi tài khoản người dùng; phân quyền truy cập tài nguyên thông tin theo đúng chức năng, nhiệm vụ được giao.
4. Thực hiện sao lưu dữ liệu trên máy chủ định kỳ; sẵn sàng phương án khắc phục sự cố, khôi phục dữ liệu khi cần thiết.
5. Tổ chức các buổi tập huấn, phổ biến kiến thức, kỹ năng về an toàn thông tin cho người dùng trong cơ quan.
6. Chủ trì, phối hợp với các phòng, đơn vị liên quan kiểm tra, xử lý các hành vi vi phạm Quy chế.

Điều 5. Trách nhiệm của người dùng

1. Tuân thủ tuyệt đối các quy định trong Quy chế này.
2. Chịu trách nhiệm cá nhân về việc bảo mật thông tin tài khoản được cấp và mọi hoạt động phát sinh từ tài khoản của mình.
3. Chủ động bảo vệ thiết bị máy tính được giao, không tự ý thay đổi cấu hình, cài đặt phần mềm trái phép.
4. Báo cáo ngay cho bộ phận phụ trách CNTT khi phát hiện các dấu hiệu bất thường, các sự cố về an toàn thông tin (máy tính nhiễm virus, nhận email nghi ngờ lừa đảo, mất thiết bị...).

5. Bàn giao đầy đủ tài khoản, dữ liệu và thiết bị CNTT cho bộ phận phụ trách CNTT khi chuyển công tác hoặc thôi việc.

CHƯƠNG III
QUY ĐỊNH CỤ THỂ

Mục 1. QUẢN LÝ MÁY TÍNH CÁ NHÂN (MÁY TRẠM)

Điều 6. Quản lý mật khẩu

1. Mật khẩu đăng nhập máy tính và các ứng dụng phải có độ dài tối thiểu 08 ký tự, bao gồm chữ hoa, chữ thường, số và ký tự đặc biệt.
2. Người dùng phải thay đổi mật khẩu định kỳ, tối thiểu 03 tháng/lần. Không được sử dụng lại các mật khẩu cũ.
3. Nghiêm cấm viết mật khẩu ra giấy để tại nơi làm việc hoặc lưu mật khẩu dưới dạng văn bản không mã hóa. Tuyệt đối không chia sẻ mật khẩu cho người khác.
4. Thiết lập chế độ tự động khóa màn hình sau 05 phút không sử dụng và bắt buộc khóa máy tính (bằng tổ hợp phím Windows + L) khi rời khỏi vị trí làm việc.

Điều 7. Quản lý phần mềm và dữ liệu

1. Chỉ được phép cài đặt và sử dụng các phần mềm có bản quyền, các phần mềm miễn phí, mã nguồn mở hợp pháp và các phần mềm chuyên ngành đã được cơ quan trang bị, cho phép.
2. Nghiêm cấm cài đặt các phần mềm không rõ nguồn gốc, phần mềm bẻ khóa (crack), các phần mềm có nguy cơ gây mất an toàn thông tin (tool hack, game online...).
3. Tất cả máy tính phải được cài đặt phần mềm diệt virus do cơ quan cung cấp, đảm bảo phần mềm luôn hoạt động và cập nhật mẫu virus mới nhất.
4. Dữ liệu công việc, văn bản, tài liệu chính thức phải được lưu trữ trên ổ đĩa mạng dùng chung đã được phân quyền. Hạn chế tối đa việc lưu trữ tài liệu quan trọng, đặc biệt là tài liệu mật trên máy tính cá nhân.

Điều 8. Sử dụng thiết bị ngoại vi và Internet

1. Chỉ sử dụng thiết bị lưu trữ ngoài (USB, ổ cứng di động) để trao đổi dữ liệu khi thực sự cần thiết. Mọi thiết bị lưu trữ ngoài phải được quét virus trước khi sử dụng.
2. Không sử dụng mạng Internet của cơ quan vào các mục đích cá nhân, giải trí làm ảnh hưởng đến hiệu suất công việc và an ninh hệ thống. Nghiêm cấm truy cập các trang web có nội dung độc hại, phản động, đồi trụy, cờ bạc.

Mục 2. QUẢN LÝ HỆ THỐNG MÁY CHỦ VÀ MẠNG

Điều 9. Quản lý truy cập máy chủ

1. Việc truy cập, quản trị hệ thống máy chủ phải tuân thủ nguyên tắc "quyền tối thiểu", chỉ những người có trách nhiệm mới được cấp quyền.

2. Mọi phiên truy cập quản trị hệ thống đều phải được ghi lại nhật ký (log) và được rà soát định kỳ.

Điều 10. Quản lý hệ thống mạng và Wi-Fi

1. Hệ thống mạng không dây (Wi-Fi) được chia thành 02 vùng riêng biệt: a) **"SNV-NoiBo":** Dành riêng cho công chức, viên chức, người lao động của Sở, yêu cầu xác thực bằng tài khoản cá nhân. b) **"SNV-Khach":** Dành cho khách đến liên hệ công tác, có mật khẩu riêng và được tách biệt hoàn toàn với mạng nội bộ.

2. Nghiêm cấm người dùng tự ý chia sẻ mật khẩu Wi-Fi "SNV-NoiBo" cho người ngoài.

3. Nghiêm cấm tự ý lắp đặt, sử dụng các thiết bị mạng như bộ phát Wi-Fi, switch, router... khi chưa được sự đồng ý của bộ phận phụ trách CNTT.

Điều 11. Quản lý Email và truy cập từ xa

1. Hệ thống thư điện tử công vụ (...@noivu.[tinh].gov.vn) chỉ được sử dụng để trao đổi các thông tin phục vụ công việc.

2. Người dùng phải đặc biệt cẩn trọng với các email lừa đảo (phishing), không bấm vào các đường dẫn lạ, không tải về các tệp đính kèm đáng ngờ.

3. Mọi kết nối từ bên ngoài Internet vào hệ thống mạng nội bộ của Sở (để làm việc từ xa) bắt buộc phải thông qua kênh kết nối an toàn (VPN) do bộ phận phụ trách CNTT cung cấp và quản lý.

CHƯƠNG IV
PHÂN QUYỀN TRUY CẬP VÀ SỬ DỤNG

Điều 12. Nguyên tắc phân quyền

1. Việc phân quyền dựa trên vai trò, vị trí công tác và chức năng, nhiệm vụ cụ thể của từng cá nhân, đơn vị.

2. Tuân thủ nguyên tắc "cần biết", chỉ cấp quyền truy cập vào những tài nguyên, dữ liệu cần thiết để hoàn thành nhiệm vụ.

3. Bảng phân quyền sẽ được bộ phận phụ trách CNTT thiết lập và rà soát, cập nhật định kỳ hoặc khi có sự thay đổi về nhân sự, chức năng nhiệm vụ.

Điều 13. Bảng phân quyền sử dụng hệ thống máy tính và mạng

Nhóm Đối tượng	Quyền Hạn và Trách Nhiệm	Ghi chú
Nhóm 1: Lãnh đạo Sở (Giám đốc, Phó Giám đốc)	- Toàn quyền truy cập dữ liệu các phòng - Được cấp quyền truy cập từ xa (VPN). - Được ưu tiên băng thông Internet.	Chịu trách nhiệm bảo mật các thông tin mang tính chỉ đạo, điều hành.
Nhóm 2: Trưởng/Phó các phòng, đơn vị	- Quyền đọc/ghi trên thư mục dùng chung của phòng/đơn vị mình quản lý. - Quyền chỉ đọc (read-only) đối với thư mục của các phòng/đơn vị khác (nếu được cho phép). - Được cấp quyền truy cập VPN khi có yêu cầu và được phê duyệt.	Chịu trách nhiệm quản lý, phân loại dữ liệu trong phạm vi đơn vị.
Nhóm 3: Chuyên viên, Nhân viên	- Quyền đọc/ghi trên thư mục cá nhân và thư mục dùng chung của phòng/đơn vị mình. - Hạn chế quyền truy cập vào thư mục của các phòng/đơn vị khác. - Hạn chế quyền cài đặt phần mềm trên máy tính.	Chỉ được truy cập dữ liệu phục vụ trực tiếp cho công việc chuyên môn.
Nhóm 4: Bộ phận Quản trị CNTT	- Quyền quản trị cao nhất (Administrator) đối với hệ thống máy chủ, thiết bị mạng, các phần mềm ứng dụng. - Quyền cài đặt, gỡ bỏ phần mềm trên tất cả các máy trạm. - Quyền giám sát lưu lượng mạng, truy cập hệ thống.	Tuân thủ quy trình bảo mật nghiêm ngặt, chịu trách nhiệm cao nhất về kỹ thuật.
Nhóm 5: Khách (Visitor)	- Chỉ được phép truy cập mạng Wi-Fi "SNV-Khach". - Không có quyền truy cập vào bất kỳ tài nguyên nào trong mạng nội bộ (máy in, ổ đĩa mạng...).	Kết nối Internet bị giới hạn về băng thông và thời gian.

CHƯƠNG V
KHEN THƯỞNG VÀ XỬ LÝ VI PHẠM

Điều 14. Khen thưởng

Tập thể, cá nhân có thành tích xuất sắc trong việc thực hiện Quy chế, có hành động ngăn chặn, báo cáo kịp thời các nguy cơ gây mất an toàn thông tin sẽ được xem xét khen thưởng theo quy định của cơ quan.

Điều 15. Xử lý vi phạm

1. Người dùng vi phạm các quy định tại Quy chế này, tùy theo tính chất, mức độ vi phạm sẽ bị xem xét xử lý kỷ luật theo quy định về xử lý kỷ luật công chức, viên chức và các quy định pháp luật liên quan.

2. Trường hợp vi phạm gây ra thiệt hại nghiêm trọng về vật chất hoặc thông tin, người vi phạm phải chịu trách nhiệm bồi thường và có thể bị truy cứu trách nhiệm hình sự theo quy định của pháp luật.

CHƯƠNG VI
ĐIỀU KHOẢN THI HÀNH

Điều 16. Tổ chức thực hiện

1. Văn phòng Sở chủ trì, phối hợp với các phòng, đơn vị trực thuộc tổ chức triển khai, phổ biến Quy chế này đến toàn thể công chức, viên chức và người lao động của Sở.

2. Trưởng các phòng có trách nhiệm đôn đốc, nhắc nhở công chức, viên chức thuộc đơn vị mình quản lý thực hiện nghiêm túc Quy chế.

3. Đối với các đơn vị trực thuộc Sở căn cứ quy chế sử dụng máy tính Client, máy chủ (Server) và hệ thống mạng nội bộ nhằm đảm bảo an toàn thông tin tại Sở Nội vụ để xây dựng quy chế sử dụng máy tính Client, máy chủ (Server) và hệ thống mạng nội bộ tại cơ quan mình.

Điều 17. Hiệu lực thi hành

1. Quy chế này có hiệu lực thi hành kể từ ngày ký Quyết định ban hành.

2. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc hoặc cần sửa đổi, bổ sung, các đơn vị, cá nhân kịp thời phản ánh về Văn phòng Sở để tổng hợp, báo cáo Giám đốc Sở xem xét, quyết định./.