ỦY BAN NHÂN DÂN THÀNH PHỐ ĐÀ NẴNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: /QĐ-UBND	*Đà Nẵng, ngày tháng 02 năm 2026*

DỰ THẢO
Ngày 09/02/2026

QUYẾT ĐỊNH

Quy chế Vận hành Hệ thống Cổng đăng nhập tập trung (SSO Gateway) bằng tài khoản VNeID cho các Hệ thống của thành phố Đà Nẵng

CHỦ TỊCH ỦY BAN NHÂN DÂN THÀNH PHỐ ĐÀ NẴNG

Căn cứ Luật Tổ chức chính quyền địa phương số 72/2025/QH15;

Căn cứ Luật Công nghệ thông tin số 67/2006/QH11;

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13;

Căn cứ Luật An ninh mạng số 116/2025/QH15;

Căn cứ Luật Giao dịch điện tử số 20/2023/QH15;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về việc ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Nghị định số 59/2022/NĐ-CP ngày 05/9/2022 của Chính phủ quy định về định danh và xác thực điện tử;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Theo đề nghị của Giám đốc Sở Khoa học và Công nghệ tại Tờ trình số /TTr-SKHCN ngày /02/2026.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này là Quy chế Vận hành Hệ thống Cổng đăng nhập tập trung (SSO Gateway) bằng tài khoản VNeID cho các Hệ thống của thành phố Đà Nẵng.

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

Điều 3. Chánh Văn phòng Ủy ban nhân dân thành phố; Giám đốc các Sở, ban, ngành; Chủ tịch UBND các xã, phường, đặc khu và Thủ trưởng các cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Bộ Khoa học và Công nghệ;
- TT TU, TT HĐND thành phố;
- CT, các PCT UBND thành phố;
- Đoàn đại biểu Quốc hội thành phố;
- UB MTTQ VN TP, đoàn thể thành phố;
- Công an TP, BCHQS TP, BCH BĐBP TP;
- Các Sở, Ban, ngành;
- UBND các xã, phường, đặc khu;
- Công báo thành phố;
- Cổng thông tin điện tử thành phố;
- Lưu: VT, SKHCN.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Hồ Quang Bửu

binhtt26-25/02/2026 10:11:54-binhtt26-binhtt26-binhtt26

ỦY BAN NHÂN DÂN THÀNH PHỐ ĐÀ NẴNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ

Vận hành Hệ thống Cổng đăng nhập tập trung (SSO Gateway) bằng tài khoản VNeID cho các Hệ thống của thành phố Đà Nẵng

(Ban hành kèm theo Quyết định số /QĐ-UBND ngày tháng 02 năm 2026 của Chủ tịch Ủy ban nhân dân thành phố Đà Nẵng)

Chương I

QUY ĐỊNH CHUNG

Điều 1. Phạm vi, đối tượng áp dụng

1. Quy chế này quy định việc vận hành Hệ thống Cổng đăng nhập tập trung (SSO Gateway) bằng tài khoản VNeID cho các Hệ thống của thành phố Đà Nẵng.

2. Quy chế này áp dụng đối với các cơ quan, tổ chức, đơn vị, địa phương tham gia sử dụng Hệ thống Cổng đăng nhập tập trung (SSO Gateway) bằng tài khoản VNeID.

Điều 2. Nguyên tắc quản lý, vận hành

Việc quản lý, vận hành, khai thác và sử dụng Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID cho các hệ thống thông tin quy định tại Quy chế này được thực hiện theo các nguyên tắc sau:

1. Thống nhất, liên thông, đồng bộ giữa các hệ thống thông tin trên địa bàn thành phố, bảo đảm phù hợp với mô hình chính quyền địa phương hai cấp và kiến trúc Chính quyền số.

2. Bảo đảm an toàn thông tin, bảo mật dữ liệu và quản lý truy cập tập trung, có kiểm soát, phân quyền rõ ràng theo chức năng, nhiệm vụ và vị trí việc làm; đáp ứng yêu cầu xác thực, định danh điện tử bằng tài khoản VNeID theo quy định.

3. Tận dụng tối đa hạ tầng kỹ thuật, dữ liệu và phần mềm hiện có, bảo đảm khả năng kế thừa, mở rộng và tích hợp; hạn chế tối đa gián đoạn hoạt động, lãng phí nguồn lực trong giai đoạn chuyển tiếp, nâng cấp hoặc sáp nhập hệ thống.

4. Xác định rõ trách nhiệm trong quản lý, vận hành và hỗ trợ kỹ thuật, bảo đảm phân công cụ thể, minh bạch giữa đơn vị chủ quản hệ thống, đơn vị vận hành kỹ thuật và các đơn vị tham gia cung cấp, tích hợp dịch vụ.

5. Tuân thủ đầy đủ các quy định pháp luật hiện hành, các quy định của Chính

phủ, Bộ, ngành Trung ương và hướng dẫn của Ủy ban nhân dân thành phố về chuyển đổi số, chính quyền số, định danh và xác thực điện tử, cũng như bảo đảm an toàn thông tin mạng.

Điều 3. Nguyên tắc bắt buộc sử dụng xác thực tập trung

1. Các hệ thống thông tin, cơ sở dữ liệu, phần mềm, nền tảng số sử dụng ngân sách nhà nước khi triển khai mới hoặc nâng cấp phải thực hiện tích hợp với Hệ thống Cổng đăng nhập tập trung (SSO Gateway).

2. Không triển khai cơ chế xác thực riêng song song nếu không có ý kiến chấp thuận bằng văn bản của cơ quan có thẩm quyền.

3. Việc tuân thủ yêu cầu tích hợp SSO Gateway là một tiêu chí trong công tác thẩm định, nghiệm thu, đánh giá an toàn thông tin và đưa hệ thống vào vận hành chính thức.

Điều 4. Các hành vi nghiêm cấm

1. Cố tình cản trở, phá hoại, làm thay đổi dữ liệu hoặc cấu trúc của Hệ thống xác thực.

2. Sử dụng tài khoản VNeID của người khác để thực hiện giao dịch, giải quyết công việc hoặc truy cập trái phép vào dữ liệu không thuộc thẩm quyền.

3. Can thiệp trái phép vào quy trình xác thực hoặc giả mạo thông tin xác thực.

4. Tiết lộ thông tin cấu hình hệ thống, dữ liệu người dùng cho bên thứ ba khi không được phép.

Điều 5. Giải thích từ ngữ

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

1. Hệ thống Cổng đăng nhập tập trung (SSO - Single Sign-On): là nền tảng kỹ thuật cho phép người dùng sử dụng một tài khoản duy nhất để truy cập vào nhiều hệ thống thông tin, ứng dụng khác nhau trong môi trường mạng của thành phố mà không cần đăng nhập lại nhiều lần.

2. Tài khoản VNeID: là danh tính điện tử của cá nhân, tổ chức được quản lý bởi Bộ Công an, dùng để xác thực người dùng khi đăng nhập vào Cổng đăng nhập tập trung.

3. Chủ quản hệ thống: là đơn vị sở hữu, chịu trách nhiệm quản lý nhà nước đối với hệ thống (Ví dụ: Sở Khoa học và Công nghệ theo phân công).

Chương II

QUY ĐỊNH VỀ ĐẢM BẢO AN TOÀN THÔNG TIN KHI VẬN HÀNH

Điều 6. Bảo đảm an toàn hạ tầng mạng trong quá trình vận hành Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID

Đơn vị quản lý, vận hành hạ tầng mạng có trách nhiệm triển khai đầy đủ các biện pháp bảo đảm an toàn hạ tầng mạng phục vụ Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID, cụ thể như sau:

1. Quản lý hạ tầng mạng nội bộ

a) Tuân thủ các quy định về kiến trúc hệ thống, tiêu chuẩn, quy chuẩn kỹ thuật hiện hành; thực hiện cài đặt, cấu hình và tổ chức hạ tầng mạng phù hợp với các tiêu chuẩn ứng dụng công nghệ thông tin trong cơ quan nhà nước, bảo đảm an toàn thông tin, hạn chế sử dụng các mô hình mạng tiềm ẩn nguy cơ mất an toàn thông tin cao.

b) Đối với các cơ quan, đơn vị có nhiều phòng, ban, đơn vị trực thuộc làm việc tại các trụ sở khác nhau, khi triển khai kết nối trên mạng đô thị (MAN) của thành phố phải thiết lập kết nối thông qua mạng riêng ảo (Virtual Private Network – VPN) nhằm bảo đảm an toàn, bảo mật dữ liệu truyền dẫn.

c) Trang bị và vận hành thiết bị tường lửa chuyên dụng hoặc phần mềm tường lửa phù hợp để kiểm soát, ngăn chặn và phát hiện kịp thời các hành vi truy nhập trái phép, tấn công từ bên ngoài vào mạng nội bộ khi kết nối với các hệ thống, mạng bên ngoài.

d) Trường hợp thực hiện truy nhập từ xa vào mạng nội bộ để thực hiện chức năng quản trị, vận hành hệ thống, bắt buộc sử dụng các giao thức truyền thông có mã hóa như SSL/TLS, VPN hoặc các cơ chế bảo mật tương đương; đồng thời thiết lập mật khẩu có độ phức tạp cao, bảo đảm yêu cầu an toàn thông tin theo quy định.

2. Quản lý mạng không dây

a) Khi triển khai mạng không dây kết nối với mạng cục bộ thông qua các điểm truy nhập (Access Point – AP), đơn vị vận hành phải cấu hình đầy đủ các tham số bảo mật, bao gồm: tên mạng (SSID), cơ chế nhận dạng, mật khẩu có độ phức tạp cao; thực hiện kiểm soát truy nhập theo địa chỉ vật lý (MAC Address) và áp dụng cơ chế mã hóa dữ liệu tối thiểu theo chuẩn WPA2 hoặc WPA3.

b) Mật khẩu truy cập mạng không dây phải được thiết lập bảo đảm độ phức tạp theo quy định; thực hiện thay đổi mật khẩu định kỳ tối thiểu 03 tháng một lần nhằm tăng cường công tác bảo mật, phòng ngừa nguy cơ lộ, lọt thông tin.

c) Trường hợp cung cấp truy cập Internet qua mạng không dây cho khách hoặc người ngoài cơ quan, đơn vị vận hành phải thiết lập SSID riêng biệt, tách biệt hoàn toàn với mạng nội bộ; đồng thời giới hạn băng thông, phạm vi truy cập và không cho phép truy nhập vào các hệ thống thông tin nội bộ, Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID.

Điều 7. Bảo đảm an toàn máy chủ vận hành Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID

1. Yêu cầu chung đối với máy chủ

Trên hệ thống máy chủ phục vụ vận hành Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID, đơn vị chủ quản, đơn vị vận hành có trách nhiệm:

a) Hệ điều hành và phần mềm: cài đặt hệ điều hành là phần mềm có bản quyền (bao gồm phần mềm thương mại hoặc phần mềm mã nguồn mở có nguồn gốc rõ ràng, được cộng đồng hoặc tổ chức uy tín hỗ trợ). Chỉ cài đặt, kích hoạt các dịch vụ, thành phần phần mềm thực sự cần thiết cho hoạt động của hệ thống; không cài đặt các dịch vụ, ứng dụng không sử dụng hoặc không rõ nguồn gốc.

b) Cập nhật và bảo vệ truy cập: thiết lập chế độ tự động cập nhật bản vá bảo mật đối với hệ điều hành, phần mềm trung gian, ứng dụng và hệ quản trị cơ sở dữ liệu được cài đặt trên máy chủ. Thiết lập cơ chế bảo vệ truy cập, bao gồm: mật khẩu truy nhập có độ phức tạp cao; tự động khóa hoặc bảo vệ màn hình sau tối đa 10 phút không sử dụng đối với các phiên truy cập quản trị.

c) Bảo mật phần cứng: thiết lập mật khẩu bảo vệ tại lớp BIOS/UEFI của máy chủ. Vô hiệu hóa hoặc kiểm soát chặt chẽ các cổng vật lý không cần thiết (đặc biệt là cổng USB) nhằm ngăn ngừa nguy cơ sao chép, cài cắm mã độc trái phép.

d) Quản lý thiết bị lưu trữ: không sử dụng thiết bị lưu trữ cá nhân để sao chép, lưu trữ hoặc xử lý thông tin, dữ liệu của hệ thống. Trường hợp cần khôi phục dữ liệu từ máy chủ hoặc máy tính trạm bị sự cố, đơn vị quản lý phải thông báo và phối hợp với cơ quan quản lý nhà nước có thẩm quyền để được hướng dẫn, hỗ trợ theo quy định.

2. Phòng, chống mã độc: đơn vị vận hành phải cấu hình tự động cập nhật phiên bản và bản vá mới; tự động quét mã độc khi sao chép, mở tệp tin; quét toàn bộ hệ thống định kỳ tối thiểu 01 lần/tuần.

3. Giám sát tiến trình và dịch vụ: định kỳ tối thiểu 01 lần/tuần, đơn vị vận hành phải kiểm tra các tiến trình, dịch vụ đang hoạt động trên máy chủ nhằm kịp thời phát hiện dấu hiệu cài cắm phần mềm độc hại, dịch vụ trái phép hoặc hành vi bất thường.

4. Quản lý nhật ký hệ thống (logfile)

a) Thu thập và lưu trữ

- Thực hiện thu thập, quản lý và sao lưu logfile theo từng tháng.

- Thời gian lưu trữ logfile trên máy chủ hoặc thiết bị lưu trữ trực tuyến từ 06 tháng đến 12 tháng; logfile của các năm trước (tối đa 03 năm) phải được lưu trữ tại hệ thống lưu trữ độc lập.

b) Bảo đảm toàn vẹn và dung lượng

- Định kỳ tối thiểu 06 tháng/lần, kiểm tra tính toàn vẹn của logfile.

- Thực hiện giám sát dung lượng lưu trữ logfile nhằm phòng ngừa tình trạng tràn log gây ảnh hưởng đến hoạt động của hệ thống thông tin.

5. Yêu cầu đối với hệ thống lưu ký, lưu trữ: đối với hệ thống lưu ký dữ liệu hoặc hệ thống cung cấp dịch vụ lưu trữ; máy chủ cơ sở dữ liệu và máy chủ ứng dụng phải được triển khai trên các máy chủ vật lý hoặc máy chủ ảo độc lập; hệ thống phải được bảo vệ bởi các lớp an toàn thông tin bao gồm tối thiểu: tường lửa, thiết bị phòng chống tấn công từ chối dịch vụ (DDoS), hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS).

6. Cấu hình dịch vụ và cổng mạng

- Khi cung cấp dịch vụ ra môi trường mạng (theo TCP/UDP Port): chỉ cấu hình, mở các cổng mạng, giao thức và dịch vụ thực sự cần thiết cho hoạt động của hệ thống. Không cấu hình các dịch vụ ra môi trường mạng đối với máy chủ cơ sở dữ liệu.

- Thực hiện kiểm tra định kỳ danh sách cổng, dịch vụ đang mở để kịp thời đóng các cổng không sử dụng.

7. Các hành vi bị nghiêm cấm: nghiêm cấm sử dụng tài nguyên tính toán của hệ thống (máy chủ, hạ tầng mạng, cổng dịch vụ) để: đào tiền ảo; rà quét, tấn công hoặc khai thác lỗ hổng bảo mật trái phép; tham gia các hoạt động vi phạm pháp luật hoặc trái quy định trên môi trường mạng.

Điều 8. Bảo đảm an toàn ứng dụng vận hành Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID

1. Bảo đảm an toàn xác thực và danh tính điện tử

- Hệ thống phải thực hiện xác thực tập trung người dùng thông qua tài khoản VNeID hoặc các cơ chế xác thực được cơ quan có thẩm quyền cho phép, bảo đảm đúng danh tính và vai trò sử dụng.

- Mỗi người dùng chỉ được gắn với một danh tính điện tử duy nhất, tương ứng với vị trí việc làm; không cho phép sử dụng tài khoản dùng chung hoặc mạo danh.

- Thông tin xác thực, mã định danh, khóa bảo mật, mã thông báo (token) phải được quản lý tập trung, lưu trữ an toàn dưới dạng mã hóa và kiểm soát chặt chẽ quyền truy cập.

- Hệ thống phải có cơ chế kiểm soát đăng nhập bất thường, cảnh báo và ngăn chặn các hành vi có dấu hiệu tấn công, giả mạo hoặc xâm nhập trái phép.

2. Kiểm soát truy cập và phân quyền

- Hệ thống phải thực hiện phân quyền truy cập theo vai trò, chức năng và nhiệm vụ của người sử dụng; áp dụng nguyên tắc phân quyền tối thiểu.

- Chỉ cho phép truy cập quản trị, cấu hình hệ thống thông qua các kết nối mạng an toàn; giới hạn phạm vi địa chỉ mạng, thiết bị và tài khoản được phép quản trị.

- Thiết lập thời gian hiệu lực của phiên đăng nhập, tự động kết thúc phiên khi người dùng không hoạt động trong khoảng thời gian xác định nhằm hạn chế rủi ro bị chiếm quyền truy cập.

- Giới hạn số lượng kết nối đồng thời, số lần đăng nhập sai nhằm phòng ngừa tấn công từ chối dịch vụ và các hành vi lạm dụng hệ thống.

3. Quản lý nhật ký, giám sát và truy vết

- Hệ thống phải ghi đầy đủ nhật ký các hoạt động, bao gồm: đăng nhập, đăng xuất, xác thực, phân quyền, thay đổi cấu hình, lỗi hệ thống và các sự kiện bất thường.

- Nhật ký phải được lưu trữ tập trung, bảo đảm tính toàn vẹn, không bị chỉnh sửa hoặc xóa trái phép; phục vụ công tác giám sát, kiểm tra, điều tra và xử lý sự cố.

- Thời gian lưu trữ nhật ký tối thiểu theo quy định của pháp luật và yêu cầu quản lý an toàn thông tin; trường hợp cần thiết có thể kéo dài để phục vụ công tác hậu kiểm.

4. Bảo mật thông tin trao đổi và tích hợp hệ thống

- Thông tin, dữ liệu trao đổi giữa Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID với các hệ thống thông tin khác phải được mã hóa, bảo đảm an toàn trong suốt quá trình truyền dẫn.

- Việc tích hợp, kết nối hệ thống phải tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin; chỉ cho phép các hệ thống đã được thẩm định, phê duyệt kết nối.

- Không cho phép truyền, chia sẻ thông tin xác thực, mã định danh hoặc dữ liệu nhạy cảm qua các kênh không an toàn hoặc không được kiểm soát.

5. An toàn ứng dụng và mã nguồn

- Hệ thống phải có cơ chế kiểm tra, xác thực dữ liệu đầu vào và đầu ra nhằm phòng ngừa các lỗ hổng bảo mật và tấn công phổ biến.

- Ứng dụng phải được bảo vệ trước các hình thức tấn công thường gặp như: tấn công chèn mã, tấn công giả mạo yêu cầu, tấn công khai thác lỗ hổng logic ứng dụng.

- Việc phát triển, nâng cấp, chỉnh sửa mã nguồn phải tuân thủ quy trình quản lý thay đổi, được kiểm thử an toàn trước khi đưa vào vận hành chính thức.

Điều 9. Bảo đảm an toàn dữ liệu trong quá trình vận hành Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID

1. Quản lý dữ liệu định danh, tài khoản và thông tin xác thực

a) Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID chỉ lưu trữ, xử lý các dữ liệu cần thiết phục vụ cho việc xác thực, phân quyền và ghi nhận trạng thái đăng nhập; không lưu trữ thông tin vượt quá phạm vi chức năng được giao.

b) Thông tin định danh điện tử, thông tin xác thực, mã phiên làm việc, khóa bảo mật và các dữ liệu nhạy cảm khác phải được bảo vệ bằng các biện pháp mã hóa phù hợp trong quá trình lưu trữ và xử lý.

c) Không cho phép chia sẻ, chuyển giao hoặc sử dụng trái phép tài khoản, thông tin xác thực, mã khóa bảo mật của Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID dưới bất kỳ hình thức nào.

2. Sao lưu, phục hồi và bảo vệ dữ liệu hệ thống

a) Đơn vị vận hành có trách nhiệm tổ chức triển khai các giải pháp sao lưu dữ liệu định kỳ đối với dữ liệu cấu hình hệ thống, dữ liệu phân quyền, nhật ký hệ

thống và các dữ liệu vận hành quan trọng khác của Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID.

b) Dữ liệu sao lưu phải được lưu trữ an toàn, tách biệt với hệ thống chính; có phương án bảo vệ chống truy cập trái phép, mất mát hoặc hư hỏng dữ liệu.

c) Phải xây dựng và duy trì các kịch bản phục hồi dữ liệu, phục hồi hệ thống để bảo đảm khả năng khôi phục hoạt động của Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID khi xảy ra sự cố.

3. Quản lý thay đổi và toàn vẹn dữ liệu

a) Mọi thay đổi liên quan đến cấu hình hệ thống, cấu trúc dữ liệu, cơ chế xác thực, phân quyền phải được quản lý, phê duyệt theo quy trình; ghi nhận đầy đủ thông tin về nội dung thay đổi, lý do, thời gian và người thực hiện.

b) Việc phân quyền thao tác đối với dữ liệu và cấu hình hệ thống phải được kiểm soát chặt chẽ; chỉ cấp quyền cho các cá nhân, bộ phận có nhiệm vụ phù hợp.

c) Các thao tác chỉnh sửa, cập nhật hoặc hủy bỏ dữ liệu phải được ghi nhận trong nhật ký hệ thống để phục vụ công tác giám sát, kiểm tra và truy vết khi cần thiết.

4. Bảo vệ dữ liệu trong quá trình chia sẻ và tích hợp

a) Dữ liệu trao đổi giữa Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID với các hệ thống thông tin, ứng dụng khác chỉ được thực hiện trong phạm vi đã được phê duyệt và phục vụ mục đích xác thực, định danh người dùng.

b) Không chia sẻ trực tiếp thông tin xác thực, mật khẩu hoặc dữ liệu nhạy cảm cho các hệ thống tích hợp; việc trao đổi thông tin phải thông qua các cơ chế trung gian an toàn theo quy định.

5. Quản lý dữ liệu khi ngừng khai thác hoặc thay đổi phạm vi sử dụng

a) Trường hợp Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID hoặc các thành phần liên quan ngừng khai thác, đơn vị vận hành có trách nhiệm thực hiện lưu trữ dữ liệu theo quy định và xóa, hủy dữ liệu trên các hệ thống không còn sử dụng, bảo đảm không để lộ, lọt thông tin.

b) Việc xóa, hủy dữ liệu phải được thực hiện theo quy trình, có biên bản xác nhận và chịu trách nhiệm trước pháp luật.

c) Khi cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc, nghỉ hưu, ngay từ thời điểm thay đổi có hiệu lực, đơn vị quản lý cá nhân đó phải thông báo

đơn vị vận hành để điều chỉnh, thu hồi, hủy bỏ tài khoản và các tài sản liên quan (khóa, thẻ nhận dạng, tài khoản,...).

6. Quản lý thiết bị lưu trữ và phương tiện chứa dữ liệu

a) Khi thiết bị máy chủ, thiết bị lưu trữ, phương tiện chứa dữ liệu của Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID mang đi bảo hành, bảo dưỡng hoặc thanh lý, phải thực hiện các biện pháp xóa dữ liệu hoặc tháo rời thiết bị lưu trữ theo quy định.

b) Việc tiêu hủy dữ liệu phải sử dụng các giải pháp kỹ thuật phù hợp nhằm bảo đảm dữ liệu không thể phục hồi.

7. Bảo vệ dữ liệu thuộc phạm vi bí mật nhà nước

Thông tin, dữ liệu thuộc phạm vi bí mật nhà nước phát sinh trong quá trình vận hành Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID phải được quản lý, lưu trữ, khai thác và bảo vệ theo đúng quy định của pháp luật về bảo vệ bí mật nhà nước.

Điều 10. Giám sát, ghi nhật ký và bảo đảm an toàn thông tin trong vận hành Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID

1. Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID phải được tổ chức giám sát, theo dõi hoạt động thường xuyên và liên tục nhằm bảo đảm hệ thống vận hành ổn định, an toàn; kịp thời phát hiện, cảnh báo và xử lý các sự cố kỹ thuật, nguy cơ mất an toàn thông tin.

2. Nội dung giám sát hệ thống bao gồm:

- Giám sát trạng thái hoạt động của các thành phần hệ thống xác thực, máy chủ, dịch vụ tích hợp và các kết nối liên thông;

- Giám sát lưu lượng truy cập, tần suất đăng nhập, các trường hợp đăng nhập thất bại, truy cập trái phép hoặc có dấu hiệu bất thường;

- Theo dõi hiệu năng, khả năng đáp ứng, mức độ ổn định và tính sẵn sàng của dịch vụ xác thực tập trung.

- Hệ thống phải thực hiện ghi nhật ký (log) đầy đủ, chính xác và liên tục đối với các hoạt động:

+ Đăng nhập, đăng xuất, xác thực thành công hoặc không thành công;

+ Cấp phát, thay đổi, thu hồi quyền truy cập và tài khoản người dùng;

+ Các sự kiện liên quan đến an toàn thông tin, cảnh báo tấn công, vi phạm

chính sách bảo mật.

3. Nhật ký hệ thống phải được lưu trữ an toàn, bảo đảm tính toàn vẹn, không bị sửa đổi, xóa trái phép; thời gian lưu trữ nhật ký thực hiện theo quy định của pháp luật và quy định của cơ quan quản lý nhà nước có thẩm quyền.

4. Đơn vị quản lý, vận hành hệ thống có trách nhiệm:

- Phân công cán bộ theo dõi, rà soát, phân tích nhật ký hệ thống định kỳ hoặc đột xuất;

- Chủ động phát hiện, cảnh báo sớm và phối hợp xử lý các nguy cơ mất an toàn thông tin;

- Thực hiện báo cáo sự cố an toàn thông tin theo quy định hiện hành.

Chương III

QUY ĐỊNH VỀ VẬN HÀNH VÀ KHAI THÁC HỆ THỐNG

Điều 11. Phạm vi áp dụng và chức năng vận hành Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID

1. Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID là nền tảng kỹ thuật thực hiện xác thực, định danh điện tử người dùng tập trung, cho phép người dùng sử dụng một tài khoản VNeID duy nhất để truy cập, sử dụng nhiều hệ thống thông tin khác nhau trong môi trường mạng của thành phố, bảo đảm thuận tiện, an toàn thông tin và kiểm soát truy cập tập trung.

2. Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID được áp dụng đối với toàn bộ cán bộ, người dân có tài khoản VNeID và được phân quyền truy cập vào hệ thống phù hợp.

3. Việc triển khai, vận hành Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID nhằm:

- Tăng cường kiểm soát, quản lý quyền truy cập và định danh người dùng;

- Bảo đảm đồng bộ danh tính điện tử và phân quyền người dùng giữa các hệ thống thông tin;

- Nâng cao mức độ an toàn thông tin, giảm thiểu rủi ro mất an toàn dữ liệu và nâng cao hiệu quả quản lý hạ tầng công nghệ thông tin của thành phố.

Điều 12. Nguyên tắc sử dụng và vận hành Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID

1. Tất cả người dùng khi truy cập vào các hệ thống thông tin quy định tại

Điều 13 phải thực hiện đăng nhập thông qua Cổng đăng nhập tập trung bằng tài khoản VNeID. Việc bỏ qua cơ chế xác thực tập trung hoặc truy cập trực tiếp vào hệ thống khi chưa được cho phép là không được phép.

2. Mỗi cán bộ, công chức, viên chức, người lao động được sử dụng một tài khoản duy nhất, gắn với danh tính điện tử VNeID và vị trí việc làm. Nghiêm cấm việc sử dụng tài khoản dùng chung, mượn hoặc chia sẻ tài khoản dưới bất kỳ hình thức nào.

3. Người sử dụng tự chịu trách nhiệm đối với toàn bộ hoạt động truy cập và sử dụng hệ thống. Mọi hành vi đăng nhập, thao tác nghiệp vụ và phát sinh dữ liệu từ tài khoản cá nhân đều được hệ thống ghi nhận, lưu vết và sử dụng làm căn cứ phục vụ công tác kiểm tra, giám sát, xác minh trách nhiệm trong xử lý công vụ và bảo đảm an toàn thông tin.

4. Người sử dụng có trách nhiệm bảo mật thông tin xác thực, không để lộ tên tài khoản, mật khẩu hoặc thông tin đăng nhập; kịp thời thông báo cho đơn vị quản trị khi phát hiện dấu hiệu rò rỉ, mất an toàn hoặc xâm nhập trái phép.

5. Việc sử dụng và vận hành Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID phải tuân thủ các quy định của pháp luật hiện hành và hướng dẫn chuyên môn, kỹ thuật của cơ quan quản lý nhà nước có thẩm quyền.

Điều 13. Quy trình đăng ký và kết nối Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID

1. Tiếp nhận yêu cầu: các cơ quan, đơn vị có nhu cầu tích hợp đăng nhập tập trung bằng tài khoản VNeID gửi văn bản đề nghị về Sở Khoa học và Công nghệ Đà Nẵng hoặc Đơn vị vận hành, kèm theo các thông tin kỹ thuật tối thiểu bao gồm: Tên hệ thống cần tích hợp, mô tả chức năng, và Địa chỉ phản hồi (Callback URL) chính thức.

2. Cấu hình hệ thống: trong thời hạn [03-05] ngày làm việc kể từ khi tiếp nhận đủ thông tin, Đơn vị vận hành có trách nhiệm kiểm tra tính hợp lệ của Callback URL, thực hiện cấu hình trên Hệ thống Cổng đăng nhập tập trung SSO Gateway. Mọi thay đổi liên quan đến callback URL, tên miền, chứng thư số phải được thông báo bằng văn bản hoặc kênh chính thức cho đơn vị vận hành trước khi áp dụng.

3. Cấp thông tin tích hợp: sau khi cấu hình thành công, Đơn vị vận hành thực hiện trao đổi với đầu mối đơn vị cần tích hợp, ký biên bản bàn giao khóa bảo mật, cấp mã định danh ứng dụng (Client ID), khóa bảo mật (Secret Key/API Key) và

cung cấp tài liệu hướng dẫn kỹ thuật cho đơn vị yêu cầu. Client ID, Client Secret được xem là thông tin mật phục vụ xác thực hệ thống. Đơn vị được cấp có trách nhiệm quản lý, lưu trữ an toàn, không chia sẻ cho bên thứ ba. Trường hợp nghi ngờ lộ lọt phải thông báo ngay cho đơn vị vận hành để thu hồi và cấp lại.

4. Kiểm thử và vận hành: đơn vị tích hợp thực hiện kết nối theo tài liệu hướng dẫn trên môi trường kiểm thử (nếu có) trước khi triển khai chính thức. Việc tích hợp chỉ được chuyển sang chính thức khi có xác nhận đạt yêu cầu kỹ thuật từ Đơn vị vận hành. Mọi thay đổi về Callback URL sau khi đã cấu hình phải được thông báo bằng văn bản hoặc kênh trao đổi chính thức để Đơn vị vận hành cập nhật kịp thời.

Điều 14. Quản lý, tích hợp và hỗ trợ kỹ thuật vận hành Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID

1. Đơn vị được Sở Khoa học và Công nghệ giao nhiệm vụ hoặc đặt hàng là đơn vị chủ trì, chịu trách nhiệm quản lý, vận hành kỹ thuật và bảo đảm an toàn thông tin đối với Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID. Nhiệm vụ cụ thể bao gồm:

a) Quản trị hệ thống

- Quản lý tập trung dữ liệu tài khoản và khóa bảo mật;

- Thực hiện cấp phát, điều chỉnh, thu hồi và phân quyền tài khoản theo cơ cấu tổ chức và vị trí việc làm;

- Quản lý, lưu trữ nhật ký truy cập, theo dõi hoạt động và phối hợp xử lý các hành vi vi phạm.

b) Tích hợp hệ thống

- Các phần mềm, Cổng thông tin điện tử, Trang dịch vụ công của các đơn vị khi tích hợp đăng nhập VNeID phải tuân thủ chuẩn kết nối do Bộ Công an và cơ quan có thẩm quyền hướng dẫn;

- Hệ thống phải có khả năng đảm bảo an toàn thông tin, tài liệu cấp độ An toàn thông tin (Cấp độ 3 trở lên) để được cấp quyền truy cập dịch vụ tương ứng.

c) Hỗ trợ kỹ thuật

- Tổ chức đào tạo, tập huấn, hướng dẫn sử dụng hệ thống cho cán bộ kỹ thuật và người sử dụng;

- Thiết lập, duy trì các kênh hỗ trợ kỹ thuật để tiếp nhận, xử lý kịp thời các vướng mắc phát sinh trong quá trình khai thác, sử dụng hệ thống.

2. Các cơ quan, đơn vị sử dụng hệ thống có trách nhiệm

a) Cử cán bộ đầu mối phối hợp với đơn vị chủ trì trong việc cập nhật thông tin, đề xuất tích hợp và tiếp nhận hỗ trợ kỹ thuật;

b) Tổ chức quản lý, giám sát việc khai thác, sử dụng Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID tại đơn vị; kịp thời phát hiện, xử lý và báo cáo các hành vi vi phạm quy định về truy cập hoặc chia sẻ tài khoản trái phép.

Điều 15. Xử lý sự cố, vi phạm và trách nhiệm trong quá trình vận hành Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID

1. Khi xảy ra sự cố kỹ thuật, gián đoạn dịch vụ hoặc sự cố an toàn thông tin liên quan đến Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID, đơn vị quản lý, vận hành có trách nhiệm:

- Khẩn trương xác định nguyên nhân, phạm vi ảnh hưởng và mức độ sự cố;

- Triển khai ngay các biện pháp kỹ thuật cần thiết để khắc phục sự cố, bảo đảm khôi phục hoạt động của hệ thống trong thời gian sớm nhất;

- Thông báo kịp thời cho các cơ quan, đơn vị liên quan về tình trạng sự cố và phương án xử lý.

2. Trường hợp sự cố vượt quá khả năng xử lý của đơn vị vận hành hoặc có ảnh hưởng nghiêm trọng đến hoạt động của các hệ thống thông tin dùng chung, phải kịp thời báo cáo cơ quan quản lý nhà nước có thẩm quyền để phối hợp chỉ đạo, hỗ trợ xử lý theo quy định.

3. Trường hợp lỗi do hệ thống VNeID (quên mật khẩu, khóa tài khoản): hướng dẫn công dân liên hệ Tổng đài hỗ trợ của Bộ Công an hoặc Công an địa phương để xử lý.

4. Cá nhân, tổ chức vi phạm các quy định về quản lý, sử dụng và vận hành Hệ thống Cổng đăng nhập tập trung bằng tài khoản VNeID, tùy theo tính chất, mức độ vi phạm, sẽ bị áp dụng một hoặc nhiều biện pháp sau:

- Nhắc nhở, yêu cầu khắc phục, tạm thời hoặc vĩnh viễn thu hồi quyền truy cập hệ thống;

- Xử lý kỷ luật theo quy định của pháp luật về cán bộ, công chức, viên chức;

- Trường hợp gây thiệt hại hoặc có dấu hiệu vi phạm pháp luật thì bị xử lý theo quy định của pháp luật hiện hành.

5. Các cơ quan, đơn vị, tổ chức, cá nhân liên quan có trách nhiệm phối hợp, cung cấp thông tin, hồ sơ, dữ liệu phục vụ công tác kiểm tra, xác minh, xử lý sự

cố và vi phạm trong quá trình vận hành hệ thống.

Chương IV

TRÁCH NHIỆM CỦA CÁC CƠ QUAN, ĐƠN VỊ VÀ CÁ NHÂN

Điều 16. Trách nhiệm của Đơn vị quản lý, vận hành hệ thống

1. Quản lý hạ tầng kỹ thuật, đảm bảo Hệ thống Cổng đăng nhập tập trung hoạt động liên tục 24/7, thông suốt và an toàn.

2. Thực hiện xây dựng hồ sơ cấp độ ATTT, triển khai các biện pháp kỹ thuật để bảo vệ hệ thống trước các nguy cơ tấn công mạng.

3. Chủ trì kỹ thuật việc tích hợp hệ thống SSO với các phần mềm dùng chung (Quản lý văn bản, Một cửa điện tử...) và Cơ sở dữ liệu quốc gia về dân cư.

4. Xây dựng tài liệu hướng dẫn, tổ chức tập huấn và thiết lập kênh hỗ trợ kỹ thuật (Tổng đài, Email, Zalo...) để xử lý sự cố đăng nhập cho người dùng.

5. Định kỳ sao lưu dữ liệu, nhật ký truy cập để phục vụ công tác khôi phục và kiểm tra an ninh.

6. Đảm bảo tính bảo mật của quá trình chuyển giao thông tin kết nối (Key/ID) đến đúng đầu mối kỹ thuật của đơn vị đăng ký qua các kênh truyền tin an toàn.

7. Đơn vị vận hành có quyền tạm dừng hoặc từ chối kết nối đối với các hệ thống không đáp ứng yêu cầu kỹ thuật, tiềm ẩn nguy cơ mất an toàn thông tin hoặc vi phạm quy định bảo mật.

Điều 17. Trách nhiệm của các Sở, Ban, ngành, UBND các xã, phường, đặc khu, các tổ chức có yêu cầu tích hợp đăng nhập VNeID...

1. Phối hợp với Đơn vị vận hành để tích hợp các phần mềm chuyên ngành do đơn vị mình quản lý vào Cổng đăng nhập tập trung; không xây dựng hệ thống đăng nhập riêng lẻ gây lãng phí.

2. Cập nhật kịp thời danh sách, trạng thái công tác của CBCCVC thuộc quyền quản lý để hệ thống phân quyền chính xác.

3. Quán triệt cán bộ, nhân viên tuân thủ quy định đăng nhập qua VNeID; chịu trách nhiệm nếu để xảy ra mất an toàn thông tin do lỗi chủ quan của cán bộ thuộc đơn vị.

4. Chịu trách nhiệm về tính chính xác và an toàn của thông tin cung cấp cho Đơn vị vận hành. Đảm bảo địa chỉ này sử dụng giao thức bảo mật (HTTPS) và không có lỗ hổng bảo mật.

5. Bảo mật tuyệt đối các khóa bảo mật (Secret Key/API Key) được cấp. Không được chia sẻ thông tin này cho bên thứ ba không có thẩm quyền. Trường hợp nghi ngờ lộ khóa, phải thông báo ngay cho Đơn vị vận hành để thực hiện cấp mới và hủy khóa cũ.

Điều 18. Trách nhiệm của Người sử dụng (CBCCVC và Công dân)

1. Tự bảo quản tài khoản VNeID, thiết bị xác thực (điện thoại cài app VNeID) và chịu trách nhiệm pháp lý đối với mọi hoạt động diễn ra dưới tài khoản của mình.

2. Thông báo ngay cho Đơn vị vận hành hoặc cơ quan công an khi phát hiện tài khoản bị lộ, bị chiếm quyền kiểm soát hoặc có dấu hiệu đăng nhập bất thường.

3. Tuân thủ các quy trình an toàn thông tin khi tham gia vào hệ thống mạng của thành phố.

Chương V

TỔ CHỨC THỰC HIỆN

Điều 19. Chế độ báo cáo và kiểm tra

1. Đơn vị vận hành có trách nhiệm định kỳ báo cáo tình hình hoạt động, các sự cố an toàn thông tin (nếu có) và hiệu quả khai thác hệ thống SSO về Sở Khoa học và Công nghệ thành phố Đà Nẵng.

2. Các hành vi vi phạm Quy chế này tùy theo tính chất, mức độ sẽ bị xử lý kỷ luật, xử phạt hành chính hoặc truy cứu trách nhiệm hình sự theo quy định của pháp luật.

Điều 20. Điều khoản thi hành

Trong quá trình thực hiện, nếu có vướng mắc, các cơ quan, đơn vị phản ánh về Sở Khoa học và Công nghệ thành phố Đà Nẵng để tổng hợp, báo cáo và xem xét sửa đổi, bổ sung cho phù hợp./.