

**QUYẾT ĐỊNH**

**Về việc Ban hành Quy chế bảo đảm an toàn các hệ thống thông tin ngành Giáo dục và Đào tạo Hà Nội.**

**GIÁM ĐỐC SỞ GIÁO DỤC VÀ ĐÀO TẠO HÀ NỘI**

Căn cứ Quyết định số 22/2024/QĐ-UBND ngày 07/03/2024 của Ủy ban nhân dân thành phố Hà Nội về việc quy định chức năng, nhiệm vụ, quyền hạn, cơ cấu tổ chức của Sở Giáo dục và Đào tạo Hà Nội;

Căn cứ Thông tư số 42/2021/TT-BGDĐT ngày 30/12/2021 Quy định về cơ sở dữ liệu giáo dục và đào tạo;

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

Theo đề nghị của Trưởng phòng Chính trị, tư tưởng - Khoa học công nghệ, Sở Giáo dục và Đào tạo Hà Nội.

**QUYẾT ĐỊNH:**

**Điều 1.** Ban hành kèm theo quyết định này Quy chế bảo đảm an toàn các Hệ thống thông tin của ngành Giáo dục và Đào tạo Hà Nội.

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

**Điều 3.** Chánh Văn phòng, Trưởng phòng các phòng ban thuộc Sở; Trưởng phòng Giáo dục và Đào tạo quận, huyện, thị xã; Hiệu trưởng các Trường trực thuộc Sở; Giám đốc các Trung tâm Giáo dục nghề nghiệp - Giáo dục thường xuyên; Công chức, viên chức, người lao động và các cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này. /.

**Nơi nhận:**

- Như Điều 3;
- Bộ GDĐT (đề b/c)
- UBND Thành phố (đề b/c)
- Đ/c Giám đốc Sở;
- Các đ/c Phó Giám đốc Sở;
- Các Phòng thuộc Sở;
- Lưu: VT, CTTT-KHCN.



**Trần Thế Cường**

**QUY CHẾ**  
**BẢO ĐẢM AN TOÀN CÁC HỆ THỐNG THÔNG TIN**  
**CỦA NGÀNH GIÁO DỤC VÀ ĐÀO TẠO HÀ NỘI**

*(Ban hành kèm theo Quyết định số 238/QĐ-SGDĐT ngày 26 tháng 9 năm 2024  
của Sở Giáo dục và Đào tạo Hà Nội)*

**Chương I**

**QUY ĐỊNH CHUNG**

**Điều 1. Phạm vi điều chỉnh**

Quy chế này quy định bảo đảm an toàn các thông tin trong hoạt động chuyển đổi số, ứng dụng công nghệ thông tin (CNTT), vận hành, khai thác hệ thống, hạ tầng, phần mềm, dữ liệu thuộc phạm vi của ngành Giáo dục và Đào tạo Hà Nội.

**Điều 2. Đối tượng áp dụng**

1. Các đơn vị Giáo dục và Đào tạo trên địa bàn thành phố Hà Nội, bao gồm: Các Phòng thuộc Sở Giáo dục và Đào tạo; các đơn vị trực thuộc Sở Giáo dục và Đào tạo; các Phòng Giáo dục và Đào tạo quận, huyện, thị xã; các cơ sở giáo dục mầm non, giáo dục phổ thông, giáo dục nghề nghiệp, giáo dục thường xuyên (sau đây gọi tắt là cơ sở giáo dục).

2. Các công chức, viên chức và người lao động trong các cơ sở giáo dục (sau đây gọi tắt là cá nhân).

3. Các tổ chức, cá nhân có liên quan tham gia xây dựng, hỗ trợ điều hành, vận hành, khai thác thông tin trên các thông tin của ngành Giáo dục và Đào tạo Hà Nội áp dụng các quy định tại Quy chế này.

**Điều 3. Giải thích từ ngữ**

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

1. *An toàn thông tin mạng* (sau đây gọi tắt là ATTTM) là sự bảo vệ thông tin, Hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

2. *Hệ thống thông tin* (sau đây gọi tắt là HTTT) là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng.

3. *Cơ sở dữ liệu ngành giáo dục và đào tạo* (sau đây gọi tắt là CSDL Ngành) là tập hợp dữ liệu số hóa thông tin quản lý về giáo dục và đào tạo (gồm dữ liệu về trường học, dữ liệu về lớp học, dữ liệu về cán bộ quản lý cơ sở giáo dục, đội ngũ giáo viên, giảng viên, và nhân viên, dữ liệu về người học, dữ liệu về chương trình giáo dục, dữ liệu về cơ sở vật chất trường học và các dữ liệu liên quan khác) do Sở Giáo dục và Đào tạo Hà Nội quản lý.

4. *Hệ thống CSDL Ngành* là hệ thống CNTT chuyên ngành do Sở Giáo dục và Đào tạo Hà Nội xây dựng, quản lý, sử dụng thống nhất trên phạm vi toàn Thành phố, có các chức năng cơ bản phục vụ công tác báo cáo, thu thập, tổng hợp dữ liệu số hóa về giáo dục mầm non, giáo dục phổ thông và giáo dục thường xuyên từ các cơ sở giáo dục đến các cấp quản lý. Hệ thống CSDL Ngành gồm hạ tầng CNTT, phần mềm quản lý và CSDL Ngành về giáo dục mầm non, giáo dục phổ thông và giáo dục thường xuyên được thiết lập, vận hành và hoạt động trên môi trường internet tại địa chỉ <https://csdl.hanoi.edu.vn>.

5. *Mã định danh* cho một đối tượng được quản lý trên CSDL Ngành là một chuỗi ký tự dùng để định danh duy nhất cho đối tượng đó trên CSDL Ngành.

6. *Tài khoản* trên CSDL Ngành gồm hai thông tin chính là tên đăng nhập và mật khẩu được cơ quan có thẩm quyền cấp để đăng nhập, báo cáo và khai thác sử dụng cơ sở dữ liệu. Có hai loại tài khoản là tài khoản quản trị dùng để quản trị CSDL Ngành theo thẩm quyền và tài khoản khai thác sử dụng dữ liệu trên CSDL Ngành.

7. *Phần mềm độc hại* là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ HTTT hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong HTTT.

8. *Sự cố ATTTM* là việc thông tin, HTTT bị tấn công hoặc gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng (sau đây gọi tắt là sự cố).

9. *Ứng cứu sự cố ATTTM* là hoạt động nhằm xử lý, khắc phục sự cố gây mất ATTTM gồm: theo dõi, thu thập, phân tích, phát hiện, cảnh báo, điều tra, xác minh sự cố, ngăn chặn sự cố, khôi phục dữ liệu và khôi phục hoạt động bình thường của HTTT.

10. *Đầu mối ứng cứu sự cố* là bộ phận hoặc cá nhân được thành viên mạng lưới ứng cứu sự cố ATTTM quốc gia cử để thay mặt cho thành viên liên lạc và trao đổi thông tin với Cơ quan điều phối quốc gia về ứng cứu sự cố hoặc các thành viên khác trong hoạt động điều phối, ứng cứu sự cố.

11. *Cá nhân được giao phụ trách bảo đảm an toàn thông tin* là cán bộ kỹ thuật hoặc cán bộ quản lý được giao phụ trách công tác bảo đảm ATTTM cho việc triển khai, vận hành, khai thác hệ thống CNTT tại đơn vị.

12. *Bên thứ ba* là các tổ chức, cá nhân có chuyên môn được đơn vị thuê hoặc hợp tác với đơn vị nhằm cung cấp hàng hóa, dịch vụ kỹ thuật cho HTTT.

13. Các trang thiết bị, thông tin thuộc HTTT của đơn vị bao gồm:

a) Trang thiết bị vật lý: là các thiết bị CNTT, phương tiện truyền thông và các thiết bị phục vụ hoạt động cho HTTT (bao gồm cả các trang thiết bị hỗ trợ như máy tính, camera giám sát và các trang thiết bị khác theo quy định);

b) Thông tin: là các dữ liệu, tài liệu liên quan đến HTTT.

c) Phần mềm: là các phần mềm hệ thống, phần mềm tiện ích, phần mềm trung gian, hệ quản trị cơ sở dữ liệu, phần mềm ứng dụng.

#### **Điều 4. Nguyên tắc bảo đảm an toàn các HTTT.**

1. Bảo đảm ATTTM được thực hiện xuyên suốt trong các hoạt động mua sắm, nâng cấp, vận hành, bảo trì và ngừng sử dụng hạ tầng, HTTT, phần mềm, dữ liệu.

2. Trách nhiệm bảo đảm ATTTM gắn với trách nhiệm của người đứng đầu cơ quan, đơn vị và cá nhân trực tiếp liên quan.

3. Trường hợp có quy định khác tại văn bản quy phạm pháp luật, quyết định của cấp có thẩm quyền cao hơn thì áp dụng quy định tại văn bản đó.

4. Thông tin thuộc Danh mục bí mật nhà nước được bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước.

5. Việc quản lý, vận hành, khai thác sử dụng Hệ thống CSDL Ngành tuân thủ các quy định hiện hành của pháp luật và bảo đảm các nguyên tắc sau:

a) Bảo đảm tính đầy đủ, chính xác, kịp thời, thuận tiện cho khai thác, sử dụng, phục vụ công tác quản lý ngành về giáo dục

b) Các cơ quan quản lý giáo dục được sử dụng dữ liệu trên CSDL Ngành trong phạm vi phân cấp và trách nhiệm quản lý được giao

c) Các tổ chức khác khai thác và sử dụng dữ liệu phải được sự đồng ý của Sở Giáo dục và Đào tạo Hà Nội và phải thực hiện việc khai thác và sử dụng dữ liệu theo đúng mục đích, nội dung đã được cho phép và theo quy định của pháp luật hiện hành.

#### **Điều 5. Kinh phí cho việc bảo đảm an toàn, quản lý, vận hành, khai thác sử dụng các HTTT**

1. Kinh phí cho việc bảo đảm an toàn, quản lý, vận hành, khai thác sử dụng các HTTT được bố trí từ nguồn kinh phí chi sự nghiệp giáo dục và các nguồn kinh phí hợp pháp khác.

2. Kinh phí tổ chức triển khai bảo đảm an toàn, quản lý, vận hành, khai thác sử dụng các HTTT tại cơ sở giáo dục do ngân sách nhà nước bố trí theo phân cấp hàng năm.

#### **Điều 6. Quản lý trang thiết bị CNTT**

1. Các cơ sở giáo dục phải thống kê, kiểm kê trang thiết bị CNTT (trang thiết bị vật lý, thông tin, phần mềm) tối thiểu mỗi năm 01 lần. Gắn quyền sử dụng trang thiết bị CNTT cho các cá nhân hoặc bộ phận cụ thể. Cá nhân sử dụng trang thiết bị CNTT phải tuân thủ các quy định về quản lý, sử dụng, bảo đảm trang thiết bị CNTT được sử dụng đúng mục đích và an toàn.

2. Các cơ sở giáo dục có trách nhiệm kiểm tra, đánh giá mức độ an toàn đối với các trang thiết bị CNTT trước khi đưa vào sử dụng.

3. Việc quản lý, sử dụng trang thiết bị CNTT khi thực hiện các hoạt động bên ngoài trụ sở làm việc của đơn vị phải bảo đảm an toàn theo quy định của thành phố và nhà nước nhằm tránh xâm nhập trái phép, lộ lọt dữ liệu. Trường hợp làm mất hoặc lộ thông tin trên thiết bị hoặc phương tiện xử lý thông tin có chứa dữ liệu về HTTT, phải báo cáo ngay cho lãnh đạo và đơn vị/bộ phận có thẩm quyền để có biện pháp xử lý, khắc phục kịp thời.

4. Thông tin liên quan đến trang thiết bị CNTT (loại trang thiết bị, số hiệu, vị trí, thông tin bản quyền, các mô tả khác cho việc thay thế, phục hồi, khắc phục sửa lỗi nhanh) cần được lưu trữ, quản lý và cập nhật kịp thời.

5. Phân loại trang thiết bị CNTT (vật lý, thông tin, phần mềm) theo mức độ giá trị, độ nhạy cảm, tầm ảnh hưởng đối với hệ thống, tần suất sử dụng, thời gian lưu trữ để xây dựng, điều chỉnh nội quy, biện pháp kỹ thuật nghiệp vụ phù hợp (định kỳ sao lưu dữ liệu, bảo trì hệ thống,...).

6. Định kỳ hằng năm, đơn vị phải xây dựng kế hoạch kiểm tra, bảo trì, bảo dưỡng trang thiết bị CNTT. Trang thiết bị lưu trữ thông tin khi không sử dụng nữa cần phải được hủy bỏ, việc hủy bỏ bảo đảm tránh mất mát dữ liệu và không thể phục hồi.

7. Khi bên thứ ba thực hiện việc cung cấp, bảo dưỡng, sửa chữa trang thiết bị CNTT cho đơn vị, phải thực hiện việc quản lý bảo đảm an toàn thông tin của đơn vị như sau:

a) Đánh giá về năng lực kỹ thuật, nhân sự, khả năng tài chính của bên thứ ba trước khi ký kết hợp đồng cung cấp hàng hóa, dịch vụ;

b) Xác định rõ trách nhiệm, quyền hạn và nghĩa vụ của các bên về bảo đảm an toàn thông tin khi ký hợp đồng. Hợp đồng với bên thứ ba phải bao gồm các điều khoản về việc xử lý khi có vi phạm quy chế an toàn, bảo mật thông tin và trách nhiệm phải bồi thường thiệt hại của bên thứ ba trong trường hợp có thiệt hại do hành vi vi phạm của bên thứ ba gây ra;

c) Chú ý đến các vấn đề về tính bí mật, tính toàn vẹn, tính sẵn sàng, tin cậy, hiệu năng tối đa, khả năng phục hồi thảm họa, phương tiện lưu trữ của HTTT khi có sự tham gia của bên thứ ba;

d) Áp dụng các biện pháp giám sát chặt chẽ và giới hạn quyền truy cập của bên thứ ba khi cho phép truy cập vào hệ thống CNTT của đơn vị;

đ) Yêu cầu bên thứ ba chủ trì, phối hợp với đơn vị kiểm tra, đánh giá an toàn thông tin sau khi bảo dưỡng, sửa chữa trang thiết bị CNTT.

### **Điều 7. Bảo đảm ATTTM khi sử dụng máy tính**

1. Máy tính dùng để soạn thảo tài liệu mật thực hiện theo các quy định về bảo vệ bí mật nhà nước.

2. Cài đặt phần mềm xử lý phần mềm độc hại và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; khi phát hiện bất kỳ dấu hiệu nào liên quan

đến việc bị nhiễm phần mềm độc hại trên máy tính phải tắt máy và báo trực tiếp cho bộ phận chuyên trách về CNTT để được xử lý kịp thời.

3. Cá nhân chỉ cài đặt phần mềm hợp lệ; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận chuyên trách về CNTT; thường xuyên cập nhật phần mềm và hệ điều hành.

4. Cá nhân chỉ truy cập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; có trách nhiệm bảo mật tài khoản truy cập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác.

5. Cá nhân không được sử dụng máy tính của đơn vị để thâm nhập bất hợp pháp vào các mạng máy tính khác; Không tự ý lắp đặt, cài đặt các thiết bị khác khi chưa được sự đồng ý của bộ phận chuyên trách về CNTT của đơn vị.

6. Thường xuyên thay đổi mật khẩu truy cập HTTT, tối thiểu 03 tháng/lần. Khuyến khích đặt mật khẩu theo nguyên tắc: (1) mật khẩu có tối thiểu 08 ký tự, (2) mật khẩu bao gồm chữ hoa, chữ thường, số và ký tự đặc biệt.

### **Điều 8. Bảo đảm an toàn trong quá trình vận hành, khai thác sử dụng các HTTT**

#### 1. Quản lý hệ thống mạng máy tính:

a) Cài đặt, cấu hình, tổ chức hệ thống mạng theo mô hình mạng phân lớp, hạn chế sử dụng mô hình mạng ngang hàng. Các đơn vị có nhiều phòng, ban, đơn vị trực thuộc không nằm trong cùng một khu vực, cần thiết lập hệ thống mạng riêng bảo mật để bảo đảm an toàn cho mạng nội bộ;

b) Khi thiết lập mạng không dây tại đơn vị, chỉ cho phép truy cập Internet, không cho phép kết nối vào mạng nội bộ của đơn vị. Thiết bị không dây cần được thiết lập các tham số như: tên, mật khẩu, mã hóa dữ liệu... và thông báo các thông tin liên quan đến điểm truy cập để cơ quan sử dụng, thường xuyên thay đổi mật khẩu nhằm tăng cường công tác bảo mật. Cá nhân không được tự ý lắp đặt thêm thiết bị vào hệ thống mạng.

#### 2. Quản lý tài khoản truy cập hệ thống:

a) Các HTTT cần giới hạn một số hữu hạn lần đăng nhập sai liên tiếp. Tổ chức theo dõi và kiểm soát tất cả các phương pháp truy cập từ xa tới HTTT; yêu cầu người dùng đặt mật khẩu với độ an toàn cao;

b) Cá nhân sử dụng HTTT được cấp và sử dụng tài khoản truy cập với định danh duy nhất gắn với cá nhân đó; Không cung cấp thông tin tài khoản cho cá nhân khác sử dụng;

c) Trường hợp cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ chế độ, trong vòng 05 ngày làm việc sau khi có quyết định của cấp có thẩm quyền thì cơ quan, đơn vị quản lý cá nhân đó phải thông báo cho đơn vị vận hành HTTT bằng văn bản có xác nhận của thủ trưởng đơn vị để điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng đối với HTTT;

d) Tài khoản quản trị (mạng, hệ điều hành, thiết bị kết nối mạng, phần mềm, ứng dụng, cơ sở dữ liệu) phải tách biệt với tài khoản truy cập của người sử dụng thông thường. Tài khoản quản trị phải được giao đích danh cá nhân làm công tác quản trị. Hạn chế dùng chung tài khoản quản trị; Trường hợp chia sẻ tài khoản quản trị thì phải được phê duyệt bởi cấp có thẩm quyền và xác định được trách nhiệm cá nhân tại mỗi thời điểm sử dụng; Giới hạn và kiểm soát các truy cập sử dụng tài khoản quản trị: (1) Thiết lập cơ chế kiểm soát việc tạo tài khoản quản trị để bảo đảm không một tài khoản nào sử dụng được khi chưa được cấp có thẩm quyền phê duyệt; (2) Phải có biện pháp giám sát việc sử dụng tài khoản quản trị; (3) Việc sử dụng tài khoản quản trị phải được giới hạn bảo đảm chỉ có 01 truy cập quyền quản trị duy nhất, tự động thoát khỏi phiên đăng nhập khi không có hoạt động trong khoảng thời gian nhất định;

đ) Khi có yêu cầu khóa quyền truy cập HTTT của tài khoản đang hoạt động, lãnh đạo đơn vị phải yêu cầu bằng văn bản gửi đơn vị chủ quản HTTT hoặc đơn vị được giao vận hành HTTT để xem xét, thực hiện. Đơn vị vận hành HTTT có quyền khóa quyền truy cập của tài khoản trong trường hợp tài khoản đó thực hiện các hành vi tấn công hoặc để xảy ra vấn đề mất an toàn, an ninh thông tin;

e) Chủ quản HTTT chủ động xây dựng quy định quản lý tài khoản truy cập hệ thống phù hợp thực tế triển khai tại đơn vị.

3. Tổ chức quản lý tài nguyên: Kiểm tra, giám sát chức năng chia sẻ thông tin. Tổ chức cấp phát tài nguyên trên máy chủ theo danh mục thư mục cho từng phòng/ban; khuyến cáo người sử dụng cân nhắc việc chia sẻ tài nguyên cục bộ trên máy tính đang sử dụng, khi thực hiện việc chia sẻ tài nguyên cần phải sử dụng mật khẩu để bảo vệ thông tin.

4. Khai thác, sử dụng các ứng dụng, HTTT theo đúng chức năng, nhiệm vụ được giao, bảo đảm phục vụ tốt công tác chuyên môn, nghiệp vụ của đơn vị, phục vụ công dân, doanh nghiệp.

5. Trong quá trình vận hành hệ thống cần thực hiện quy định về phòng chống vi-rút, mã độc đáp ứng các yêu cầu cơ bản như:

a) Định kỳ kiểm tra, diệt vi-rút, mã độc và phương tiện mang thông tin, dữ liệu nhận từ bên ngoài trước khi sử dụng; Không mở các thư điện tử lạ, các tệp tin đính kèm hoặc các liên kết trong các thư lạ để tránh vi-rút, mã độc;

b) Không vào các trang/cổng thông tin điện tử không có nguồn gốc xuất xứ rõ ràng, đáng ngờ;

c) Báo ngay cho người quản trị hệ thống xử lý trong trường hợp phát hiện nhưng không diệt được vi-rút, mã độc;

d) Không tự ý cài đặt các phần mềm khi chưa được phép của người quản trị hệ thống.

6. Ứng dụng chữ ký số chuyên dùng để bảo đảm an toàn, an ninh thông tin trong việc triển khai ứng dụng CNTT trong hoạt động cơ quan nhà nước và phục vụ công dân, tổ chức.

## **Chương II**

### **QUẢN LÝ VÀ KHAI THÁC, SỬ DỤNG CSDL NGÀNH**

#### **Điều 9. Tài khoản trên CSDL Ngành**

Tài khoản trên CSDL Ngành được cấp cho tổ chức, cá nhân dùng để quản trị, báo cáo dữ liệu, khai thác và sử dụng thông tin từ CSDL Ngành.

1. Tài khoản quản trị CSDL Ngành do Sở Giáo dục và Đào tạo quản lý.
2. Tài khoản quản trị của các cơ sở giáo dục do Sở Giáo dục và Đào tạo cấp và giao cho các cơ sở giáo dục quản lý, sử dụng.
3. Tài khoản khai thác sử dụng của các Phòng thuộc Sở Giáo dục và Đào tạo do Sở Giáo dục và Đào tạo cấp, giao cho các Phòng, cá nhân quản lý, sử dụng.
4. Tài khoản quản trị của các phòng Giáo dục và Đào tạo do Sở Giáo dục và Đào tạo cấp và giao cho các Phòng Giáo dục và Đào tạo quản lý, sử dụng. Tài khoản khai thác sử dụng của các đơn vị, cá nhân thuộc và trực thuộc Phòng Giáo dục và Đào tạo do Phòng Giáo dục và Đào tạo cấp, giao cho các đơn vị, cá nhân quản lý, sử dụng.
5. Tài khoản quản trị của các cơ sở giáo dục do Sở Giáo dục và Đào tạo hoặc Phòng Giáo dục và Đào tạo trực tiếp quản lý cấp và giao cho các cơ sở giáo dục quản lý, sử dụng. Tài khoản khai thác sử dụng của các bộ phận, cá nhân trong cơ sở giáo dục do cơ sở giáo dục cấp và giao cho bộ phận, cá nhân quản lý, sử dụng.
6. Tổ chức, cá nhân được giao tài khoản chịu trách nhiệm bảo mật tài khoản, bảo mật dữ liệu và quản lý, sử dụng tài khoản theo đúng mục đích, chức năng quy định.

#### **Điều 10. Mã định danh trên CSDL Ngành**

1. Sở Giáo dục và Đào tạo quy định mã định danh các đối tượng quản lý trên CSDL Ngành sử dụng thống nhất trong ngành giáo dục bao gồm: Phòng Giáo dục và Đào tạo và các cơ sở giáo dục, giáo viên, giảng viên, cán bộ quản lý giáo dục, nhân viên và người học. Mã định danh của cơ sở giáo dục do Sở Giáo dục và Đào tạo hoặc Phòng Giáo dục và Đào tạo trực tiếp quản lý cấp từ lần tạo lập thông tin đầu tiên về cơ sở giáo dục đó trên CSDL Ngành.
2. Mã định danh của mỗi đối tượng được quản lý trên CSDL Ngành là duy nhất, được hình thành từ lần nhập dữ liệu đầu tiên và bất biến (không bị thay đổi hoặc xóa bỏ từ khi mã được sinh ra), được dùng thống nhất, xuyên suốt ở tất cả các cấp học. Mã định danh phục vụ công tác quản lý, báo cáo, kết nối dữ liệu trên CSDL Ngành và các mục đích khác do Bộ Giáo dục và Đào tạo quy định.
3. Trường hợp cơ sở giáo dục không còn hoạt động, Sở Giáo dục và Đào tạo hoặc Phòng Giáo dục và Đào tạo trực tiếp quản lý chỉ thay đổi thông tin trạng thái của cơ sở giáo dục, không xóa mã định danh và hồ sơ trên CSDL Ngành.



4. Trường hợp giáo viên, giảng viên, cán bộ quản lý và nhân viên chuyên công tác, ngừng làm việc hoặc thôi việc, cơ sở giáo dục cập nhật trạng thái và thông tin hồ sơ điện tử, không xóa hồ sơ và mã định danh trên CSDL Ngành.

5. Trường hợp người học tạm dừng học, thôi học, chuyển đi, cơ sở giáo dục và các cơ quan liên quan chỉ cập nhật trạng thái hồ sơ điện tử của người học, không xóa hồ sơ trên CSDL Ngành.

### **Điều 11. Báo cáo dữ liệu trên CSDL Ngành**

1. Nội dung báo cáo, kỳ báo cáo, thời hạn báo cáo dữ liệu trên CSDL Ngành được thực hiện theo quy định về chế độ báo cáo thống kê ngành giáo dục và khi có yêu cầu của Sở Giáo dục và Đào tạo.

2. Việc báo cáo dữ liệu trên CSDL Ngành được thực hiện qua tài khoản đã được cung cấp hoặc qua trực tích hợp dữ liệu theo hướng dẫn của Sở Giáo dục và Đào tạo.

3. Sở Giáo dục và Đào tạo có trách nhiệm tổ chức hướng dẫn, đôn đốc việc triển khai báo cáo và quản lý dữ liệu thuộc phạm vi quản lý trên cơ sở dữ liệu giáo dục và đào tạo; chịu trách nhiệm và bảo đảm dữ liệu đầy đủ, chính xác và báo cáo đúng thời hạn theo yêu cầu của Bộ Giáo dục và Đào tạo.

4. Phòng Giáo dục và Đào tạo có trách nhiệm tổ chức hướng dẫn, đôn đốc việc triển khai báo cáo và quản lý dữ liệu thuộc phạm vi quản lý trên CSDL Ngành; bảo đảm dữ liệu đầy đủ, chính xác và báo cáo đúng thời hạn theo yêu cầu của Sở Giáo dục và Đào tạo và các cơ quan có thẩm quyền.

5. Các cơ sở giáo dục mầm non, giáo dục phổ thông, giáo dục thường xuyên có trách nhiệm quản lý và tổ chức cập nhật báo cáo dữ liệu lên CSDL Ngành; bảo đảm dữ liệu đầy đủ, chính xác và báo cáo đúng thời hạn theo yêu cầu của Sở Giáo dục và Đào tạo và các cơ quan có thẩm quyền.

### **Điều 12. Quản lý, vận hành, khai thác sử dụng Hệ thống CSDL Ngành**

1. Thông tin trong CSDL Ngành được sử dụng thống nhất trên toàn Thành phố, có giá trị pháp lý trong quản lý giáo dục và đào tạo.

2. Hình thức khai thác sử dụng thông tin trong CSDL Ngành được thực hiện thông qua tài khoản được cấp, qua trực kết nối trao đổi dữ liệu hoặc văn bản.

3. Việc sử dụng thông tin trong CSDL Ngành phải tuân thủ các quy định của pháp luật về sở hữu dữ liệu và bảo vệ an toàn thông tin cá nhân.

4. Sở Giáo dục và Đào tạo, Phòng Giáo dục và Đào tạo và các cơ quan quản lý giáo dục và các cơ sở giáo dục được khai thác sử dụng thông tin trong phạm vi quản lý; ban hành quy định nội bộ về quản lý, sử dụng, khai thác dữ liệu, trong đó quy định cụ thể trách nhiệm quản lý và khai thác sử dụng thông tin từ các tài khoản người dùng; tiếp nhận và xử lý những góp ý, khiếu nại đối với dữ liệu trong thẩm quyền quản lý.

5. Các cơ quan, tổ chức, cá nhân ngoài ngành giáo dục có nhu cầu sử dụng thông tin từ CSDL Ngành thực hiện theo quy định của pháp luật về tiếp cận thông tin.

**Điều 13. Hướng dẫn, hỗ trợ kỹ thuật sử dụng cơ sở dữ liệu giáo dục và đào tạo**

1. Sở Giáo dục và Đào tạo cung cấp tài liệu điện tử về hướng dẫn sử dụng và các tài liệu liên quan phục vụ nhu cầu tập huấn, hướng dẫn sử dụng cơ sở dữ liệu giáo dục và đào tạo của người dùng; tiếp nhận thông tin yêu cầu hỗ trợ kỹ thuật và hướng dẫn sử dụng được thực hiện qua địa chỉ thư điện tử [csdl@hanoiedu.vn](mailto:csdl@hanoiedu.vn).

2. Việc tổ chức hướng dẫn, hỗ trợ kỹ thuật sử dụng CSDL Ngành tại các địa bàn do Phòng Giáo dục và Đào tạo và cơ sở giáo dục thực hiện theo điều kiện và nhu cầu.

3. Trong quá trình sử dụng, nếu phát hiện sự cố kỹ thuật liên quan đến CSDL Ngành, các cơ sở giáo dục, các Phòng Giáo dục và Đào tạo, các sở giáo dục và đào tạo tổng hợp, báo cáo về Sở Giáo dục và Đào tạo để có biện pháp xử lý kịp thời.

### Chương III

#### TỔ CHỨC THỰC HIỆN

**Điều 14. Trách nhiệm của cá nhân trong các cơ sở giáo dục**

1. Trách nhiệm của cá nhân được giao phụ trách an toàn thông tin:

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

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

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

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

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

2. Trách nhiệm của cá nhân tham gia:

a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin. Chịu trách nhiệm bảo đảm ATTTM trong phạm vi trách nhiệm và quyền hạn được giao;

b) Mỗi cá nhân phải có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản được giao sử dụng.

c) Khi phát hiện nguy cơ hoặc sự cố mất ATTTM phải báo cáo ngay với lãnh đạo và bộ phận chuyên trách CNTT của đơn vị để kịp thời ngăn chặn và xử lý;

d) Tham gia các chương trình đào tạo, hội nghị về ATTTM được các đơn vị phụ trách về ATTTM tổ chức.

### **Điều 15. Trách nhiệm của các cơ sở giáo dục**

1. Giám đốc, Thủ trưởng cơ sở giáo dục chịu trách nhiệm về tính chính xác, đầy đủ, kịp thời về dữ liệu của đơn vị mình quản lý trong CSDL Ngành.

2. Giám đốc, Thủ trưởng các cơ sở giáo dục chịu trách nhiệm trước Giám đốc Sở nếu lơ là trong công tác bảo đảm ATTTM, để xảy ra hậu quả, thiệt hại nghiêm trọng tại đơn vị thuộc phạm vi quản lý.

3. Giám đốc, Thủ trưởng các cơ sở giáo dục có trách nhiệm tổ chức thực hiện các quy định tại quy chế này và chịu trách nhiệm trong công tác bảo đảm ATTTM của đơn vị mình. Phân công một bộ phận hoặc cá nhân chuyên trách bảo đảm an toàn thông tin của đơn vị, tạo điều kiện để các cá nhân phụ trách an toàn thông tin được học tập, nâng cao trình độ về an toàn thông tin.

4. Xây dựng quy định, quy trình khai thác dữ liệu cho các phần mềm ứng dụng, CSDL Ngành; quy chế, quy trình nội bộ về bảo đảm an toàn thông tin, ứng cứu sự cố phù hợp với quy chế này, các quy định của pháp luật và tình hình từng đơn vị.

5. Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả.

6. Chủ động phối hợp đơn vị chuyên trách về ATTTM trong việc duy trì kết nối, chia sẻ đầy đủ dữ liệu giám sát theo thời gian thực để được hỗ trợ giám sát, phân tích, cảnh báo sớm về các nguy cơ về ATTTM và tấn công mạng.

### **Điều 16. Trách nhiệm của Sở Giáo dục và Đào tạo**

1. Trách nhiệm của Bộ phận chuyên trách CNTT Sở Giáo dục và Đào tạo

a) Có trách nhiệm tham mưu với Ban Giám đốc Sở về công tác bảo đảm ATTTM trong ngành Giáo dục và Đào tạo thành phố Hà Nội; tổ chức triển khai hỗ trợ, giải đáp người dùng của các cơ sở giáo dục.

b) Tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin, làm đầu mối liên hệ và phối hợp với Đội ứng cứu sự cố ATTTM thành phố Hà Nội.

c) Tổng hợp và báo cáo về tình hình ATTTM định kỳ gửi Sở Thông tin và Truyền thông, UBND Thành phố, Bộ Giáo dục và Đào tạo và các đơn vị có liên quan theo quy định.

đ) Chịu trách nhiệm xây dựng và phối hợp triển khai các chương trình bồi dưỡng về ATTTM, tổ chức các hội nghị, hội thảo chuyên đề và tuyên truyền về an toàn thông tin ngành Giáo dục và Đào tạo.

## 2. Trách nhiệm của các Phòng thuộc Sở Giáo dục và Đào tạo

a) Chịu trách nhiệm bảo đảm ATTTM của đơn vị, tổ chức phổ biến, nâng cao nhận thức, trách nhiệm của mỗi cá nhân trong đơn vị thực hiện nghiêm túc các nội dung đã nêu trong Quy chế này.

b) Chịu trách nhiệm về tính chính xác, đầy đủ, kịp thời của dữ liệu thuộc phạm vi, chức năng và lĩnh vực phụ trách.

## **Điều 17. Trách nhiệm thi hành**

1. Chánh Văn phòng, Chánh Thanh tra, Trưởng các phòng thuộc Sở Giáo dục và Đào tạo, Trưởng phòng Giáo dục và Đào tạo các quận, huyện, thị xã, người đứng đầu các cơ sở giáo dục chịu trách nhiệm thi hành Quy chế này.

2. Trong quá trình triển khai thực hiện, nếu có khó khăn, vướng mắc, Chánh Thanh tra, Trưởng các phòng thuộc Sở Giáo dục và Đào tạo, Trưởng phòng Giáo dục và Đào tạo các quận, huyện, thị xã, Thủ trưởng các đơn vị trực thuộc Sở Giáo dục và Đào tạo phản ánh bằng văn bản về Văn phòng Sở để tổng hợp, báo cáo Giám đốc Sở Giáo dục và Đào tạo xem xét, sửa đổi, bổ sung kịp thời./.