QUY CHẾ
Quản lý, vận hành, khai thác và sử dụng hệ thống thông tin, cơ sở dữ liệu của Trường Cao đẳng Sơn La

(ban hành kèm theo Quyết định số /QĐ-CĐSL ngày 28/8/2025)

Chương I. QUY ĐỊNH CHUNG

Điều 1. Mục đích

1. **Bảo vệ dữ liệu**

- Bảo vệ dữ liệu cá nhân của viên chức, người lao động, sinh viên, học sinh, học viên; ngăn ngừa việc thu thập, sử dụng, tiết lộ trái phép.

- Bảo vệ dữ liệu quản lý, dữ liệu đào tạo, dữ liệu thi cử, hồ sơ hành chính, tài chính, nhân sự của Trường.

2. **Đảm bảo an toàn hệ thống**

- Đảm bảo an toàn, an ninh hệ thống CNTT, bao gồm: máy chủ, mạng nội bộ, hệ thống học trực tuyến, phần mềm quản lý đào tạo, email công vụ, website của Trường.

- Ngăn chặn, hạn chế tối đa các rủi ro: mất dữ liệu, lộ lọt thông tin, tấn công mạng, truy cập trái phép.

3. **Xác định trách nhiệm**

- Quy định rõ trách nhiệm của từng cấp quản lý (Ban Giám hiệu, Phòng HC-QT, các phòng nghiệp vụ, khoa, phòng khác) trong việc quản lý, vận hành, khai thác và bảo vệ hệ thống thông tin, cơ sở dữ liệu.

- Quy định trách nhiệm của từng cá nhân (Viên chức, người lao động, sinh viên, học sinh) trong việc bảo mật tài khoản, sử dụng dữ liệu đúng mục đích, báo cáo sự cố kịp thời.

4. **Tuân thủ pháp luật**

- Đảm bảo việc quản lý, vận hành hệ thống thông tin và cơ sở dữ liệu tuân thủ Luật An toàn thông tin mạng 2015, Luật An ninh mạng 2018, Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, và các văn bản chỉ đạo của Bộ GD&ĐT.

5. **Nâng cao nhận thức**

- Góp phần nâng cao ý thức, trách nhiệm của Viên chức, người lao động, sinh viên, học sinh về bảo mật dữ liệu và an toàn thông tin.

- Tạo nền tảng xây dựng môi trường số an toàn, phục vụ chuyển đổi số giáo dục.

Điều 2. Đối tượng áp dụng và nguyên tắc áp dụng

1. **Trong nội bộ Trường**

- Ban Giám hiệu, các phòng chức năng, khoa, trung tâm, bộ môn.

- Viên chức, người lao động.

- Sinh viên, học sinh, học viên hệ chính quy, vừa học vừa làm, đào tạo ngắn hạn, trực tuyến.

2. **Đối tác, đơn vị bên ngoài**

- Các doanh nghiệp, tổ chức, cá nhân có hợp đồng hoặc thỏa thuận hợp tác cung cấp dịch vụ CNTT, phần mềm, hạ tầng, đào tạo trực tuyến, tư vấn bảo mật cho Trường.

- Các chuyên gia, cộng tác viên được Trường mời tham gia vào quá trình quản trị, vận hành, bảo trì hệ thống thông tin hoặc đào tạo tập huấn về an toàn thông tin.

3. **Nguyên tắc áp dụng**

- Tất cả các đối tượng nêu trên phải chấp hành nghiêm Quy chế này và các quy định pháp luật có liên quan.

- Trường hợp đối tác, doanh nghiệp không tuân thủ, Trường có quyền chấm dứt hợp tác và yêu cầu bồi thường theo quy định.

Chương II. QUẢN LÝ, VẬN HÀNH HỆ THỐNG

Điều 3. Phân cấp trách nhiệm

1. **Ban Giám hiệu**

- Chịu trách nhiệm cao nhất về an toàn, bảo mật và quản lý toàn bộ HTTT/CSDL

2. Ban hành, phê duyệt quy định, quy trình; quyết định xử lý sự cố nghiêm trọng.

3. **Phòng Hành chính – Quản trị (HC-QT)**

- Quản lý hạ tầng CNTT, an toàn vật lý, sao lưu dữ liệu.

4. Giám sát, phát hiện và xử lý sự cố kỹ thuật; phối hợp tập huấn, tuyên truyền về an toàn thông tin.

5. **Phòng Đào tạo, Phòng Khảo thí & Đảm bảo chất lượng, Phòng Tổ chức cán bộ & Công tác HSSV**

- Quản lý dữ liệu nghiệp vụ (đào tạo, khảo thí, hồ sơ cán bộ – sinh viên).

- Đảm bảo dữ liệu chính xác, kịp thời; phối hợp với Phòng HC-QT về an toàn và tính toàn vẹn dữ liệu.

6. **Các khoa, phòng, trung tâm khác**

- Nhập và quản lý dữ liệu thuộc lĩnh vực chuyên môn; chịu trách nhiệm về độ chính xác, đầy đủ.

- Viên chức, người lao động, sinh viên, học sinh

- Sử dụng đúng tài khoản được cấp, bảo mật mật khẩu và dữ liệu truy cập.

- Báo cáo kịp thời khi phát hiện sự cố, vi phạm.

Điều 4. Quản lý tài khoản và truy cập

1. **Cấp phát tài khoản**

- Mỗi viên chức, người lao động, sinh viên, học sinh, học viên được cấp 01 tài khoản định danh riêng gắn với mã số viên chức hoặc mã sinh viên.

- Tài khoản chỉ có giá trị sử dụng trong thời gian làm việc/học tập tại Trường.

2. **Quản lý mật khẩu**

- Mật khẩu phải có tối thiểu 8 ký tự, bao gồm chữ hoa, chữ thường, số và ký tự đặc biệt.

- Người dùng phải thay đổi mật khẩu **ít nhất 3 tháng/lần** hoặc ngay khi phát hiện nguy cơ bị lộ.

- Không được sử dụng mật khẩu dễ đoán (ngày sinh, số điện thoại, tên…).

3. **Thu hồi tài khoản**

- Khi viên chứ nghỉ việc, sinh viên thôi học hoặc tốt nghiệp, Phòng HC-QT có trách nhiệm thu hồi/khóa tài khoản trong vòng **07 ngày**.

- Các dữ liệu liên quan phải được chuyển giao cho phòng ban phụ trách trước khi thu hồi tài khoản.

4. **Theo dõi truy cập**

- Toàn bộ hoạt động đăng nhập, khai thác dữ liệu đều được hệ thống ghi nhật ký (log).

- Log phải lưu giữ tối thiểu 12 tháng để phục vụ kiểm tra, điều tra khi cần.

Điều 5. Vận hành hệ thống

1. **Hạ tầng kỹ thuật**

- Hệ thống CNTT của Trường phải có **UPS, tường lửa, phần mềm chống virus, hệ thống phát hiện xâm nhập (IDS/IPS)**.

- Các máy chủ, thiết bị mạng phải được bảo dưỡng định kỳ ít nhất 1 lần/năm.

2. **Sao lưu dữ liệu**

- **Hằng ngày**: dữ liệu đào tạo, thi cử, hệ thống học trực tuyến.

- **Hằng tuần**: dữ liệu hành chính, tài chính, nhân sự.

- Bản sao lưu phải được lưu ở ít nhất 2 nơi (máy chủ chính và thiết bị dự phòng).

3. **Cập nhật và bảo mật**

- Phần mềm, hệ điều hành, ứng dụng phải được cập nhật bản vá bảo mật kịp thời.

- Không cài đặt phần mềm lạ, không rõ nguồn gốc lên hệ thống máy chủ.

- Tài khoản quản trị hệ thống phải được bảo mật nghiêm ngặt, chỉ cấp cho người được Hiệu trưởng ủy quyền.

4. **Vận hành liên tục**

- Phòng HC-QT chịu trách nhiệm đảm bảo hệ thống hoạt động liên tục, hạn chế tối đa thời gian gián đoạn.

- Trường hợp phải dừng hệ thống để bảo trì, Phòng HC-QT phải thông báo trước cho các đơn vị liên quan.

Chương III. BẢO VỆ DỮ LIỆU CÁ NHÂN

Điều 6. Phạm vi dữ liệu cá nhân

1. **Dữ liệu cá nhân cơ bản** do Trường quản lý, bao gồm nhưng không giới hạn:

- Thông tin định danh: họ tên, ngày sinh, giới tính, quốc tịch, mã số viên chức/sinh viên/học sinh, số CCCD/hộ chiếu.

- Thông tin liên hệ: địa chỉ, số điện thoại, email.

- Thông tin học tập: kết quả học tập, điểm rèn luyện, nhận xét đánh giá.

- Thông tin hành chính: hồ sơ tuyển sinh, hồ sơ viên chức, quyết định công tác, khen thưởng, kỷ luật.

2. **Dữ liệu cá nhân nhạy cảm**, bao gồm:

- Thông tin tài chính: học phí, học bổng, trợ cấp, tài khoản ngân hàng.

- Thông tin sức khỏe, hồ sơ y tế (nếu có).

- Thông tin chính trị, quan điểm, hoạt động đoàn thể, tôn giáo (nếu được lưu giữ).

- Thông tin định danh số: chữ ký số, tài khoản truy cập hệ thống nội bộ.

3. **Nguyên tắc phân loại và bảo mật**

- Dữ liệu cơ bản: được quản lý, khai thác trong phạm vi chuyên môn của từng phòng ban.

- Dữ liệu nhạy cảm: chỉ được xử lý khi thật sự cần thiết, có thẩm quyền phê duyệt, áp dụng biện pháp bảo mật cao (mã hóa, hạn chế quyền truy cập).

Điều 7. Nguyên tắc thu thập, lưu trữ và xử lý

1. **Nguyên tắc chung**

- Việc thu thập dữ liệu cá nhân phải **có mục đích rõ ràng**, phục vụ công tác đào tạo, quản lý, khảo thí, nghiên cứu hoặc theo yêu cầu pháp luật.

- Không được thu thập quá phạm vi cần thiết; mọi hành vi thu thập ngoài mục đích phải được Hiệu trưởng phê duyệt.

2. **Lưu trữ dữ liệu**

- Dữ liệu điện tử phải được lưu trên hệ thống máy chủ của Trường hoặc dịch vụ lưu trữ được phê duyệt, có cơ chế bảo mật.

- Hồ sơ giấy (tuyển sinh, viên chức, tài chính…) phải được lưu giữ tại kho hồ sơ của Phòng chức năng, có niêm phong, kiểm soát ra vào.

3. **Xử lý dữ liệu**

- Việc xử lý (sửa, cập nhật, xóa, chia sẻ) phải do đơn vị có thẩm quyền thực hiện.

- Mọi hoạt động xử lý phải được ghi nhận trong hệ thống quản lý (log).

4. **Thời hạn lưu trữ**

- Thực hiện theo quy định pháp luật, quy định của Bộ GD&ĐT và lưu trữ nội bộ của Trường.

- Khi hết thời hạn, dữ liệu phải được hủy theo quy trình an toàn (xóa an toàn, tiêu hủy hồ sơ giấy).

Điều 8. Quyền của chủ thể dữ liệu

1. **Quyền được biết**: được thông báo khi dữ liệu được thu thập, mục đích và phạm vi xử lý.

2. **Quyền truy cập và chỉnh sửa**: được yêu cầu cập nhật, chỉnh sửa, bổ sung thông tin khi có sai lệch.

3. **Quyền xóa dữ liệu**: được yêu cầu hủy bỏ dữ liệu khi không còn mục đích xử lý hợp pháp, trừ trường hợp pháp luật yêu cầu lưu giữ.

4. **Quyền phản đối**: có quyền phản đối việc sử dụng dữ liệu cá nhân ngoài phạm vi đã thông báo.

5. **Quyền khiếu nại, tố cáo**: được quyền gửi đơn khiếu nại, tố cáo nếu phát hiện hành vi vi phạm bảo mật dữ liệu cá nhân; được bảo vệ danh tính khi khiếu nại.

Điều 9. Trách nhiệm bảo vệ dữ liệu cá nhân

1. **Phòng HC-QT**

- Đảm bảo an toàn kỹ thuật cho dữ liệu: áp dụng biện pháp mã hóa, phân quyền truy cập, giám sát log hệ thống.

- Quản lý máy chủ, thiết bị lưu trữ, bảo đảm dữ liệu không bị truy cập trái phép.

2. **Phòng Đào tạo, Phòng Khảo thí & ĐBCL, Phòng TC-CB & CT HSSV**

- Quản lý dữ liệu nghiệp vụ trong phạm vi: hồ sơ đào tạo, điểm, ngân hàng đề, kết quả thi, hồ sơ viên chức, hồ sơ học sinh - sinh viên.

- Chịu trách nhiệm nhập liệu chính xác, kịp thời; đối soát dữ liệu định kỳ.

3. **Các khoa, phòng, trung tâm khác**

- Chịu trách nhiệm về dữ liệu chuyên môn do đơn vị nhập (ví dụ: kết quả nghiên cứu, học phí, hoạt động ngoại khóa).

- Không tự ý chia sẻ dữ liệu ra ngoài khi chưa được phép.

4. Viên chức, người lao động, sinh viên, học sinh

- Chỉ sử dụng dữ liệu trong phạm vi quyền hạn.

- Không được mua bán, tiết lộ, phát tán dữ liệu cá nhân dưới bất kỳ hình thức nào.

- Có trách nhiệm bảo mật tài khoản, mật khẩu; thông báo ngay khi phát hiện sự cố, nguy cơ rò rỉ dữ liệu.

Chương IV. AN TOÀN HỆ THỐNG CNTT

Điều 10. Biện pháp kỹ thuật bảo đảm an toàn hệ thống

1. Phòng HC-QT chịu trách nhiệm vận hành hạ tầng kỹ thuật, đảm bảo các máy chủ, hệ thống mạng, thiết bị CNTT hoạt động ổn định.

2. Các biện pháp kỹ thuật cơ bản phải được áp dụng, bao gồm:

- Tường lửa bảo vệ hệ thống mạng.
- Phần mềm chống virus, chống mã độc cho máy chủ và máy trạm.
- Cập nhật hệ điều hành, phần mềm thường xuyên để vá lỗ hổng bảo mật.
- Sao lưu dữ liệu định kỳ và lưu trữ an toàn.

3. Phòng TC-CB & CT HSSV phối hợp tham mưu Ban Giám hiệu về chính sách quản lý dữ liệu cá nhân và quy trình sử dụng hệ thống thông tin an toàn.

4. Các khoa, phòng, trung tâm phải tuân thủ hướng dẫn kỹ thuật của Phòng HC-QT, đồng thời quản lý, bảo mật dữ liệu trong phạm vi phụ trách.

Điều 11. Sao lưu và khôi phục dữ liệu

1. Phòng HC-QT chịu trách nhiệm thực hiện sao lưu dữ liệu:

2. Bản sao lưu phải được lưu trữ ở ít nhất 02 nơi: máy chủ chính và thiết bị dự phòng (ổ cứng ngoài, lưu trữ đám mây nếu có điều kiện).

3. Ít nhất 01 lần/năm, Phòng HC-QT kiểm tra khả năng phục hồi dữ liệu từ bản sao lưu.

4. Phòng TC-CB & CT HSSV phối hợp giám sát quá trình khôi phục dữ liệu, đảm bảo dữ liệu cá nhân và hồ sơ sinh viên, cán bộ được bảo toàn đầy đủ.

Điều 12. Giám sát và kiểm tra định kỳ

1. Giám sát thường xuyên

- Cán bộ phụ trách CNTT (thuộc Phòng HC-QT) có trách nhiệm theo dõi hoạt động hệ thống hằng ngày: nhật ký truy cập, đăng nhập trái phép, dung lượng lưu trữ, hiệu năng máy chủ, sao lưu dữ liệu.
- Khi phát hiện bất thường, báo cáo ngay cho Trưởng phòng HC-QT và đồng thời thông báo Phòng TC-CB & CT HSSV để phối hợp.

2. Kiểm tra định kỳ

- **Phòng HC-QT và Phòng TC-CB & CT HSSV phối hợp tham mưu Ban Giám hiệu** tổ chức kiểm tra nội bộ **ít nhất 1 lần/năm** về công tác an toàn thông tin, bảo vệ dữ liệu cá nhân.
- Nội dung kiểm tra tập trung vào:

+ Quản lý, phân quyền và sử dụng tài khoản truy cập.

+ Việc tuân thủ quy định bảo mật dữ liệu cá nhân trong các phòng, khoa, trung tâm.

+ Tình trạng sao lưu dữ liệu và các biện pháp kỹ thuật cơ bản bảo đảm an toàn hệ thống.

- Khi cần thiết, tham mưu Ban Giám hiệu mời chuyên gia/cơ quan chức năng hỗ trợ kiểm tra chuyên sâu.

3. Diễn tập xử lý sự cố

- Nhà trường khuyến khích tổ chức **diễn tập giả định trên giấy/tình huống mô phỏng** (ví dụ: giả định rò rỉ dữ liệu sinh viên, sự cố mất máy chủ).

- Phòng HC-QT chuẩn bị tình huống kỹ thuật; Phòng TC-CB & CT HSSV chuẩn bị nội dung về quy trình, báo cáo và xử lý vi phạm.

- Khi có điều kiện, hai phòng tham mưu Ban Giám hiệu mời chuyên gia bên ngoài tổ chức diễn tập thực tế.

4. Báo cáo kết quả

- Sau mỗi đợt kiểm tra hoặc diễn tập, **Phòng HC-QT và Phòng TC-CB & CT HSSV** phối hợp lập báo cáo gửi Ban Giám hiệu.

- Báo cáo gồm: tình hình hệ thống, mức độ tuân thủ, sự cố phát sinh (nếu có), kết quả xử lý và kiến nghị giải pháp tăng cường.

Điều 13. Xử lý sự cố an toàn thông tin

1. Phát hiện sự cố

- Sự cố an toàn thông tin bao gồm nhưng không giới hạn: tấn công mạng, xâm nhập trái phép, nhiễm mã độc, lộ/lọt/mất dữ liệu, sự cố hạ tầng (mất điện, hỏng máy chủ, sự cố đường truyền), sử dụng tài khoản trái phép.

- Viên chức, người lao động, sinh viên, học sinh khi phát hiện sự cố phải báo cáo ngay cho Phòng Hành chính – Quản trị (HC-QT).

2. Xử lý ban đầu (do Phòng HC-QT chủ trì)

- Nhanh chóng **cô lập hệ thống**, khoanh vùng sự cố, ngắt kết nối máy chủ, thiết bị hoặc tài khoản bị ảnh hưởng để tránh lan rộng.

- Ghi nhận, lưu trữ **nhật ký hệ thống (log)** và các bằng chứng liên quan để phục vụ điều tra.

- Thực hiện các biện pháp kỹ thuật khẩn cấp: diệt virus, ngăn chặn truy cập, thay đổi mật khẩu, khôi phục tạm thời.

3. Báo cáo

- Phòng HC-QT có trách nhiệm báo cáo Hiệu trưởng và Ban Giám hiệu **trong vòng 24 giờ** kể từ khi phát hiện sự cố, nêu rõ:

+ Loại sự cố; thời gian, địa điểm phát hiện.

+ Mức độ ảnh hưởng, phạm vi tác động.

+ Biện pháp xử lý ban đầu đã triển khai.

- Trường hợp sự cố nghiêm trọng, Ban Giám hiệu chỉ đạo phối hợp với cơ quan chức năng (Cục An ninh mạng & phòng chống tội phạm sử dụng CNTT – Bộ Công an, Bộ GD&ĐT) và gửi báo cáo chính thức **trong vòng 72 giờ** theo quy định pháp luật.

4. Phối hợp xử lý

- Các phòng, khoa, đơn vị có liên quan phải cung cấp đầy đủ thông tin, dữ liệu khi được yêu cầu, phối hợp xác minh nguyên nhân và hậu quả.

- Phòng Đào tạo, Phòng Khảo thí & ĐBCL, Phòng Tổ chức cán bộ & Công tác HSSV chịu trách nhiệm kiểm tra tính toàn vẹn dữ liệu nghiệp vụ thuộc phạm vi quản lý.

- Các khoa, phòng khác rà soát dữ liệu chuyên môn, báo cáo kịp thời sai lệch (nếu có).

5. Khắc phục và khôi phục hệ thống

- Sau khi cô lập và xử lý, Phòng HC-QT tổ chức khôi phục hệ thống từ bản sao lưu an toàn, đảm bảo dữ liệu không bị mất mát.

- Thực hiện đối soát với các phòng nghiệp vụ để xác nhận dữ liệu đã được khôi phục đầy đủ, chính xác.

6. Rút kinh nghiệm và phòng ngừa

- Sau mỗi sự cố, Phòng HC-QT phối hợp với các đơn vị liên quan lập **báo cáo tổng kết**, đánh giá nguyên nhân, trách nhiệm, hậu quả và đề xuất biện pháp phòng ngừa.

- Tổ chức phổ biến bài học kinh nghiệm cho các đơn vị, viên chức, sinh viên, học sinh để tránh lặp lại sự cố tương tự.

Chương V. HỢP ĐỒNG CNTT VÀ CAM KẾT BẢO MẬT

Điều 14. Hợp đồng công nghệ thông tin (CNTT)

1. Nguyên tắc chung

- Mọi hợp đồng CNTT (triển khai phần mềm, dịch vụ học trực tuyến, quản lý đào tạo, quản lý hồ sơ sinh viên, dịch vụ máy chủ, dịch vụ lưu trữ dữ liệu, bảo trì hệ thống…) ký kết giữa Trường Cao đẳng Sơn La và đơn vị cung cấp dịch vụ phải tuân thủ quy định của pháp luật và có điều khoản bảo mật dữ liệu bắt buộc.

- Quyền sở hữu toàn bộ dữ liệu hình thành, phát sinh trong quá trình sử dụng dịch vụ thuộc về **Trường Cao đẳng Sơn La**. Nhà cung cấp không được sử dụng dữ liệu này cho mục đích khác.

2. Nội dung tối thiểu của hợp đồng CNTT

a) **Quyền sở hữu và trách nhiệm dữ liệu**

- Quyền sở hữu toàn bộ thông tin, dữ liệu (bao gồm dữ liệu cá nhân của viên chức, sinh viên; dữ liệu đào tạo, khảo thí, hành chính, tài chính) thuộc về Trường.

- Nhà cung cấp chỉ được xử lý dữ liệu trong phạm vi mục đích hợp đồng, không được sao chép, chia sẻ, chuyển giao dữ liệu cho bên thứ ba khi chưa có văn bản chấp thuận.

b) **Yêu cầu về bảo mật và an toàn hệ thống**

- Nhà cung cấp phải áp dụng các biện pháp kỹ thuật và tổ chức phù hợp nhằm bảo vệ dữ liệu cá nhân theo Nghị định 13/2023/NĐ-CP, Luật An toàn thông tin mạng 2015 và Luật An ninh mạng 2018.

- Có trách nhiệm đảm bảo an toàn hệ thống, bảo vệ chống xâm nhập, mã độc, mất dữ liệu trong suốt quá trình cung cấp dịch vụ.

- Cam kết duy trì tính toàn vẹn, đầy đủ, chính xác của dữ liệu.

c) **Cam kết chuyển giao dữ liệu**

- Khi hợp đồng kết thúc hoặc bị chấm dứt, nhà cung cấp có trách nhiệm bàn giao **toàn bộ dữ liệu** cho Trường bằng hình thức an toàn (bản gốc, đầy đủ, có khả năng sử dụng ngay).

- Nhà cung cấp không được giữ lại bất kỳ bản sao nào sau khi đã bàn giao.

d) **Chế độ báo cáo sự cố**

- Nhà cung cấp có trách nhiệm thông báo ngay cho Trường trong vòng 24 giờ kể từ khi phát hiện sự cố liên quan đến dữ liệu hoặc an toàn hệ thống.

- Phối hợp với Trường để báo cáo cơ quan chức năng trong vòng 72 giờ nếu sự cố nghiêm trọng theo quy định.

e) **Chế tài vi phạm hợp đồng**

- Nếu nhà cung cấp vi phạm, để xảy ra mất mát, lộ lọt, sử dụng sai mục đích dữ liệu, Trường có quyền:

+ Chấm dứt hợp đồng ngay lập tức.

+ Yêu cầu bồi thường toàn bộ thiệt hại về vật chất và tinh thần.

+ Đưa nhà cung cấp vào danh sách hạn chế hợp tác trong tương lai.

+ Trường hợp có dấu hiệu vi phạm pháp luật, chuyển hồ sơ cho cơ quan chức năng.

3. Trách nhiệm phối hợp

- Nhà cung cấp có trách nhiệm phối hợp chặt chẽ với Phòng HC-QT và các phòng ban của Trường trong quá trình vận hành, bảo trì, khắc phục sự cố.

Điều 15. Cam kết bảo mật nội bộ

1. Đối tượng phải cam kết

- Tất cả viên chức, người lao động, người lao động trong Trường.

- Tất cả sinh viên, học viên có quyền truy cập và sử dụng hệ thống thông tin, cơ sở dữ liệu của Trường.

- Các cá nhân được Trường cấp quyền truy cập dữ liệu trong thời gian làm việc, học tập, nghiên cứu.

2. Hình thức cam kết

- Ký **"Cam kết bảo mật dữ liệu"** theo mẫu (Phụ lục 1).

- Bản cam kết được lưu giữ tại Phòng Tổ chức cán bộ & Công tác HSSV (đối với viên chứ, nhân viên) và tại phòng/khoa quản lý học sinh, sinh viên (đối với sinh viên).

- Cam kết có giá trị trong suốt thời gian công tác, học tập tại Trường và còn ràng buộc trách nhiệm đối với dữ liệu đã tiếp cận sau khi nghỉ việc, thôi học.

3. Nội dung cam kết tối thiểu

- Không chia sẻ tài khoản, mật khẩu cho người khác; phải bảo mật mật khẩu và thay đổi định kỳ theo quy định.

- Không sao chép, trích xuất, tiết lộ, chuyển giao dữ liệu cho bên thứ ba khi chưa được phép bằng văn bản của Trường.

- Chỉ sử dụng dữ liệu đúng mục đích công vụ, học tập, nghiên cứu được giao.

- Có trách nhiệm báo cáo ngay cho đơn vị phụ trách (Phòng HC-QT hoặc phòng nghiệp vụ liên quan) khi phát hiện sự cố, nguy cơ rò rỉ dữ liệu, hành vi truy cập trái phép.

- Chấp hành đầy đủ quy định pháp luật (Nghị định 13/2023/NĐ-CP, Luật An toàn thông tin mạng, Luật An ninh mạng) và các quy chế nội bộ của Trường.

4. Trách nhiệm khi vi phạm cam kết

- Cá nhân vi phạm cam kết bảo mật sẽ bị xử lý theo Điều 17 của Quy chế này và các quy định pháp luật hiện hành.

- Tùy mức độ vi phạm, có thể bị:

+ Nhắc nhở, cảnh cáo, xử lý kỷ luật nội bộ.

+ Buộc thôi việc đối với viên chức, người lao động nếu vi phạm nghiêm trọng.

+ Kỷ luật buộc thôi học hoặc đình chỉ đối với sinh viên.

+ Chuyển hồ sơ cho cơ quan chức năng để truy cứu trách nhiệm hình sự trong trường hợp vi phạm đặc biệt nghiêm trọng.

Chương VI. BÁO CÁO VÀ XỬ LÝ VI PHẠM

Điều 16. Báo cáo

1. Báo cáo định kỳ hằng năm

- Tất cả các phòng, khoa, trung tâm, đơn vị trực thuộc Trường có trách nhiệm **báo cáo hằng năm** về công tác quản lý, vận hành, bảo mật hệ thống thông tin và cơ sở dữ liệu thuộc phạm vi quản lý.

- Nội dung báo cáo gồm:

+ Tình hình quản lý, khai thác, sử dụng hệ thống thông tin, cơ sở dữ liệu trong năm.

+ Đánh giá việc tuân thủ quy định về bảo vệ dữ liệu cá nhân, sử dụng tài khoản, mật khẩu, phân quyền truy cập.

+ Các sự cố, vi phạm (nếu có) và biện pháp khắc phục đã thực hiện.

+ Kế hoạch, đề xuất cho năm tiếp theo.

- Báo cáo gửi về **Phòng Hành chính – Quản trị** (tổng hợp kỹ thuật) và **Phòng Tổ chức cán bộ & Công tác HSSV** (tổng hợp nghiệp vụ) trước ngày 15 tháng 12 hằng năm; hai phòng này tổng hợp, trình **Ban Giám hiệu** xem xét.

2. Báo cáo đột xuất/khẩn cấp

- Khi phát hiện sự cố hoặc vi phạm (lộ lọt dữ liệu, tấn công mạng, truy cập trái phép, mua bán dữ liệu, sử dụng sai mục đích…), đơn vị/cá nhân có liên quan phải **báo cáo ngay trong vòng 24 giờ** kể từ khi phát hiện.

- Nội dung báo cáo khẩn gồm:

+ Thời gian, địa điểm, hình thức phát hiện sự cố.

+ Mô tả sơ bộ sự cố/vi phạm.

+ Đối tượng dữ liệu bị ảnh hưởng.

+ Biện pháp xử lý ban đầu đã thực hiện.

- Báo cáo gửi trực tiếp đến **Phòng HC-QT** (xử lý kỹ thuật) và đồng thời báo cáo **Ban Giám hiệu**.

- Trường hợp sự cố nghiêm trọng, Ban Giám hiệu chỉ đạo Phòng HC-QT phối hợp các đơn vị liên quan **báo cáo cơ quan chức năng trong vòng 72 giờ** theo quy định.

3. Hình thức báo cáo

- Báo cáo định kỳ hằng năm: bằng văn bản chính thức (có chữ ký, đóng dấu của đơn vị) và file điện tử.

- Báo cáo khẩn: có thể gửi qua email công vụ để kịp thời xử lý, sau đó bổ sung văn bản chính thức.

Nguyên tắc chung

- Mọi hành vi vi phạm quy định về quản lý, vận hành, khai thác và sử dụng HTTT, CSDL; vi phạm quy định pháp luật về bảo vệ dữ liệu cá nhân, an toàn thông tin mạng đều bị xử lý nghiêm minh.

- Việc xử lý căn cứ vào tính chất, mức độ, hậu quả của hành vi vi phạm và đối tượng vi phạm.

Đối với viên chứ, nhân viên, học sinh, sinh viên

a) **Vi phạm nhẹ** (sơ suất, lần đầu, chưa gây hậu quả nghiêm trọng):

- Nhắc nhở, phê bình bằng văn bản.

- Yêu cầu khắc phục ngay hành vi vi phạm.

b) **Vi phạm trung bình** (vi phạm nhiều lần, gây ảnh hưởng đến dữ liệu hoặc hệ thống ở mức hạn chế):

- Xử lý kỷ luật theo quy định của Trường (cảnh cáo, khiển trách).

- Ghi vào đánh giá, xếp loại thi đua cuối năm.

c) **Vi phạm nghiêm trọng** (cố ý tiết lộ, làm lộ lọt dữ liệu nhạy cảm, mua bán dữ liệu, phá hoại hệ thống, gây thiệt hại tài sản, uy tín Trường):

- Buộc thôi việc đối với cán bộ, nhân viên.

- Buộc thôi học hoặc kỷ luật ở mức cao nhất đối với sinh viên.

- Chuyển hồ sơ cho cơ quan chức năng để **truy cứu trách nhiệm hình sự** theo quy định pháp luật.

Đối với đơn vị cung cấp dịch vụ CNTT

a) **Vi phạm hợp đồng ở mức nhẹ** (không đảm bảo chất lượng dịch vụ, chậm tiến độ, thiếu biện pháp kỹ thuật an toàn):

- Nhắc nhở, cảnh cáo bằng văn bản.

- Yêu cầu khắc phục trong thời hạn quy định.

b) **Vi phạm nghiêm trọng** (làm mất dữ liệu, để lộ lọt dữ liệu cá nhân, không chuyển giao dữ liệu khi kết thúc hợp đồng, sử dụng dữ liệu trái phép):

- **Chấm dứt hợp đồng ngay lập tức**.

- **Bồi thường toàn bộ thiệt hại** phát sinh cho Trường theo quy định pháp luật.

- Bị đưa vào danh sách hạn chế hợp tác trong tương lai.

- Trường hợp vi phạm pháp luật, hồ sơ sẽ được chuyển cơ quan chức năng để xử lý hình sự.

- **Trách nhiệm liên đới**

- Người đứng đầu đơn vị để xảy ra vi phạm do thiếu kiểm tra, giám sát cũng bị xem xét trách nhiệm.

- Các cá nhân, tổ chức liên quan nếu tiếp tay, bao che vi phạm cũng bị xử lý theo quy định.

Chương VII. TỔ CHỨC THỰC HIỆN

Điều 18. Tổ chức thực hiện

1. Phòng Hành chính – Quản trị (HC-QT)

- Là đầu mối **tham mưu cho Ban Giám hiệu** về công tác quản lý, vận hành hạ tầng CNTT, đảm bảo an toàn hệ thống.

- Quản lý, duy trì hoạt động ổn định của **máy chủ, mạng, thiết bị CNTT**; thực hiện sao lưu, dự phòng và khôi phục dữ liệu khi có sự cố.

- Triển khai, giám sát các **biện pháp kỹ thuật bảo mật**: tường lửa, phần mềm diệt virus, hệ thống phát hiện xâm nhập.

- Theo dõi nhật ký truy cập hệ thống, kịp thời phát hiện và xử lý hành vi truy cập trái phép.

- Tổng hợp, báo cáo định kỳ và đột xuất cho Ban Giám hiệu về tình hình vận hành, sự cố kỹ thuật, vi phạm an toàn thông tin.

2. Phòng Đào tạo, Phòng Khảo thí & Đảm bảo chất lượng, Phòng Tổ chức cán bộ & Công tác HSSV

- **Phòng Đào tạo**: Quản lý và vận hành hệ thống đào tạo, học trực tuyến; nhập, cập nhật và kiểm tra dữ liệu về chương trình học, kết quả học tập của sinh viên.

- **Phòng Khảo thí & ĐBCL**: Quản lý ngân hàng đề thi, dữ liệu thi cử, kết quả đánh giá; bảo đảm tính chính xác, minh bạch; chịu trách nhiệm bảo mật dữ liệu thi.

- **Phòng Tổ chức cán bộ & Công tác HSSV**: Quản lý dữ liệu hồ sơ viên chức; hồ sơ sinh viên (tuyển sinh, học bổng, kỷ luật, rèn luyện, chính sách…); đảm bảo dữ liệu cập nhật kịp thời và đúng quy trình.

- Các phòng này phối hợp với Phòng HC-QT trong việc phân quyền truy cập, giám sát sử dụng, xử lý sự cố phát sinh.

- Định kỳ thực hiện **đối soát dữ liệu** với các đơn vị có liên quan để bảo đảm tính chính xác và đầy đủ.

3. Các khoa, phòng, trung tâm trực thuộc

- Có trách nhiệm **nhập liệu và cập nhật dữ liệu** liên quan đến lĩnh vực chuyên môn do đơn vị phụ trách (ví dụ: Khoa nhập điểm chuyên môn, Phòng Tài chính nhập dữ liệu học phí, Trung tâm nhập dữ liệu hoạt động bồi dưỡng…).

- Đảm bảo dữ liệu do mình nhập lên hệ thống **đúng, đủ, kịp thời**, không được tự ý xóa, chỉnh sửa dữ liệu ngoài phạm vi thẩm quyền.

- Phối hợp với các phòng nghiệp vụ chính (Đào tạo, Khảo thí & ĐBCL, TCCB & CT HSSV) để **đối soát, xác nhận dữ liệu** định kỳ.

- Cử cán bộ phụ trách đầu mối liên hệ với Phòng HC-QT khi có sự cố hoặc yêu cầu kỹ thuật.

4. Viên chức, người lao động, sinh viên, học sinh

- Chỉ sử dụng tài khoản cá nhân được cấp, tuyệt đối không chia sẻ cho người khác.

- Có trách nhiệm bảo mật mật khẩu, thay đổi định kỳ, không truy cập trái phép vào dữ liệu không thuộc quyền hạn.

- Chịu trách nhiệm về mọi hành vi thao tác trên hệ thống bằng tài khoản của mình.

- Báo cáo ngay cho đơn vị quản lý hoặc Phòng HC-QT trong vòng 24h khi phát hiện sự cố hoặc hành vi vi phạm.

Điều 19. Tuyên truyền, tập huấn và nâng cao nhận thức

1. Phòng Tổ chức Cán bộ & Công tác HSSV (TCCB & CT HSSV)

- Tham mưu cho Ban Giám hiệu về kế hoạch, nội dung, hình thức tuyên truyền - phổ biến - tập huấn liên quan đến an toàn, an ninh thông tin.
- Chủ trì xây dựng chương trình tập huấn theo từng đối tượng (viên chức, người lao động kỹ thuật, sinh viên).
- Tổ chức triển khai các buổi truyền thông nội bộ, tuần sinh hoạt công dân - sinh viên, hoặc lồng ghép trong các sự kiện, hội thảo của Trường.
- Phối hợp với các đơn vị khác để chuẩn bị tài liệu, biểu mẫu đánh giá, và thu thập phản hồi sau mỗi đợt tập huấn.

*** Phòng TCCB-HSSV tham mưu giảng dạy/Tập huấn chuyên sâu tối thiểu các nội dung:** An toàn thông tin, bảo mật dữ liệu, quản trị mạng, phòng chống tấn công mạng; Quy định pháp luật về bảo vệ dữ liệu cá nhân, an toàn thông tin; Bảo mật dữ liệu đào tạo, khảo thí, hồ sơ cán bộ & HSSV; Kỹ năng nhận diện email giả mạo, phần mềm độc hại…

2. Phòng Hành chính – Quản trị (HC-QT)

- Đảm bảo hạ tầng CNTT, trang thiết bị (máy chiếu, âm thanh, mạng, đường truyền, phần mềm hỗ trợ) cho các hoạt động tập huấn.
- Thiết lập, giám sát, và khắc phục sự cố kỹ thuật trong suốt quá trình tổ chức.
- Hỗ trợ an toàn vật lý và an ninh hệ thống khi diễn ra các hoạt động trực tuyến (online training, webinar).
- Phối hợp với TCCB & CT HSSV trong việc lập lịch, sắp xếp địa điểm, bố trí phòng học/hội trường.

3. Các đơn vị, khoa, phòng, trung tâm có trách nhiệm triển khai các nội dung theo phụ lục.

Phụ lục 1. Cam kết bảo mật dữ liệu (Viên chức, người lao động, sinh viên, học sinh)

Phụ lục 2. Cam kết bảo mật dữ liệu (nhà cung cấp dịch vụ cntt)

Phụ lục 3. Sơ đồ/ma trận phân công trách nhiệm

Phụ lục 4. Mẫu báo cáo sự cố/vi phạm bảo mật dữ liệu