UBND TỈNH SƠN LA
TRƯỜNG CAO ĐẲNG SƠN LA
Số: 339 / KH-CĐSL

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc
Sơn La, ngày 13 tháng 10 năm 2025

KẾ HOẠCH
Tăng cường đảm bảo an ninh mạng, bảo mật thông tin, an toàn dữ liệu tại Trường Cao đẳng Sơn La

1. Căn cứ triển khai

Căn cứ Luật An ninh mạng số 24/2018/QH14

Căn cứ theo Nghị định 53/2022/NĐ-CP ngày 15/8/2022 về quy định chi tiết một số điều của luật an ninh mạng

Căn cứ theo công văn số 35-CV/TU ngày 03/10/2025 của Thường trực Tỉnh ủy Sơn La về việc thực hiện Thông báo số 06-TB/CQQTTBCĐ ngày 27/9/2025 của Cơ quan thường trực BCĐ Trung ương;

Căn cứ Công văn số 375-CV/ĐU ngày 06/10/2025 của Đảng ủy Ủy ban nhân dân tỉnh Sơn La về việc thực hiện 35-CV/TU ngày 03/10/2025 của Thường trực Tỉnh ủy Sơn La

2. Mục đích, yêu cầu

2.1. Mục đích

Bảo vệ an ninh quốc gia và trật tự an toàn xã hội: Bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. Kế hoạch này là hoạt động nhằm bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội trên không gian mạng.

Thực hiện nghiêm túc các quy định pháp luật: Triển khai hoạt động bảo vệ an ninh mạng đối với hệ thống thông tin theo quy định của Luật An ninh mạng số 24/2018/QH14 và Nghị định 53/2022/NĐ-CP.

Xây dựng không gian mạng lành mạnh: Xây dựng không gian mạng lành mạnh, không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

Củng cố lòng tin số và nâng cao nhận thức: Củng cố lòng tin số của người dân (bao gồm học sinh, sinh viên) khi hoạt động, tương tác, làm việc trên không gian mạng, đồng thời tiếp tục triển khai công tác tuyên truyền, phổ biến để nâng cao nhận thức về bảo đảm an ninh mạng.

2.2. Yêu cầu

Nguyên tắc chủ động phòng ngừa: Phải thực hiện nghiêm việc bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu là nhiệm vụ trọng yếu, thường xuyên. Đồng thời,

phải lấy phòng ngừa chủ động là chính, đi trước một bước, không để bị động, bất ngờ trong mọi tình huống.

Tuân thủ pháp luật và nguyên tắc: Phải tuân thủ Hiến pháp và pháp luật; bảo đảm lợi ích của Nhà nước, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

Kết hợp nhiệm vụ chặt chẽ: Kết hợp chặt chẽ giữa nhiệm vụ bảo vệ an ninh mạng, bảo vệ hệ thống thông tin với nhiệm vụ phát triển kinh tế - xã hội, bảo đảm quyền con người, quyền công dân.

Kiểm tra và đánh giá nghiêm ngặt: Hệ thống thông tin, đặc biệt là Hệ thống thông tin quan trọng về an ninh quốc gia (nếu có), phải được thẩm định, chứng nhận đủ điều kiện về an ninh mạng trước khi đưa vào vận hành, sử dụng; và phải thường xuyên kiểm tra, giám sát về an ninh mạng trong quá trình sử dụng.

Gắn kết quả công tác cán bộ: Đưa kết quả đánh giá chỉ số bảo đảm an ninh mạng của cơ quan, tổ chức vào các tiêu chí đánh giá tín nhiệm, năng lực của cán bộ, đặc biệt là người đứng đầu (Ban Giám hiệu, Trưởng Khoa/Phòng) để xếp loại cán bộ hàng năm.

Xử lý kịp thời: Mọi hành vi vi phạm pháp luật về an ninh mạng phải được xử lý kịp thời, nghiêm minh.

3. Nội dung, phân công thực hiện

3.1 Hoàn thiện Cơ chế Lãnh đạo, Trách nhiệm và Quy định Nội bộ

STT	Nội dung	Căn cứ Pháp lý (Chủ yếu)	Thời gian kế tiếp/Ghi chú	ĐV thực hiện
1.	Ban hành Nghị quyết chuyên đề và Quy định nội bộ: Ban hành Nghị quyết của Đảng ủy và Quy định sử dụng, quản lý, bảo đảm an ninh mạng máy tính nội bộ và mạng Internet của Trường.	CV 357 Mục 1; Luật ANM Điều 23; NĐ 53 Điều 23	Thực hiện theo văn bản hướng dẫn từ cấp trên (Tỉnh ủy/UBND tỉnh)	
2.	Phân tách mạng (Nếu có bí mật nhà nước): Thực hiện kiểm tra và đảm bảo mạng máy tính nội bộ có lưu trữ bí mật nhà nước được tách biệt vật lý hoàn toàn với mạng kết nối Internet.	NĐ 53 Điều 23; Luật ANM Điều 17	Quý IV/2025	Phòng TC& CTHSSV
3.	Tích hợp tiêu chí đánh giá cán bộ: Đưa kết quả đánh giá chỉ số bảo đảm an ninh mạng vào các tiêu chí đánh giá tín nhiệm, năng lực của cán bộ, đặc biệt là người đứng đầu (Ban Giám hiệu, Trưởng Khoa/Phòng) để xếp loại cán bộ	CV 357 Mục 1	Phối hợp: Ban Tổ chức Đảng ủy, Bộ phận Chuyên trách An ninh mạng (IT). Thời gian: Hoàn tất việc tham mưu/xây dựng bổ sung tiêu chí trong	Phòng TC& CTHSSV

	hàng năm.		Quý IV/2025.	
4.	Thiết lập Chế tài xử lý vi phạm: Bổ sung chế tài xử lý những vi phạm quy định về đảm bảo an ninh mạng vào Quy định nội bộ của Trường.	NĐ 53 Điều 23, khoản 2 (e); Luật ANM Điều 9	**Thời gian:** Hoàn tất việc xây dựng chế tài và tích hợp vào Quy định nội bộ cùng thời điểm hành động 1 (theo hướng dẫn của cơ quan cấp trên).	Phòng TC& CTHSSV

3.2. Nguyên tắc Phòng ngừa Chủ động và Biện pháp Kỹ thuật

Nhiệm vụ: Lấy phòng ngừa chủ động là chính, đi trước một bước, không để bị động, bất ngờ trong mọi tình huống.

STT	Nội dung	Căn cứ Pháp lý (Chủ yếu)	Thời gian kế tiếp/Ghi chú	ĐV thực hiện
5.	Ban hành Phương án Bảo đảm An ninh mạng: Ban hành Phương án bảo đảm an ninh mạng đối với hệ thống thông tin, bao gồm quy định về thẩm định an ninh mạng và kiểm tra, đánh giá an ninh mạng.	NĐ 53 Điều 24	Thường xuyên	Phòng HC-QT
6.	Giám sát kỹ thuật và Phân vùng mạng: Triển khai phân tách mạng thành các vùng khác nhau (máy chủ, DMZ, mạng nội bộ) và thiết lập giải pháp kiểm soát, phát hiện và ngăn chặn truy cập không tin cậy.	NĐ 53 Điều 11; Luật ANM Điều 14	Thường xuyên	Phòng HC-QT
7.	Quản lý Nhật ký và Truy cập Quản trị: Thiết lập cơ chế ghi và lưu trữ nhật ký về hoạt động hệ thống và người dùng tối thiểu 3 tháng. Đồng thời, giới hạn và kiểm soát việc sử dụng tài khoản có quyền quản trị.	NĐ 53 Điều 11	Thường xuyên: Triển khai công cụ tập trung hóa nhật ký và chính sách quản trị truy cập.	Phòng HC-QT
8.	Thiết lập Dự phòng Dữ liệu (Sao lưu): Đảm bảo dữ liệu phát sinh phải được sao lưu trong vòng 24 giờ và dữ liệu sao lưu phải được kiểm tra khả năng khôi phục định kỳ 6 tháng một lần.	NĐ 53 Điều 11	Liên tục: Thực hiện sao lưu. Định kỳ 6 tháng: Kiểm tra khả năng khôi phục.	Phòng HC-QT

3.3. Ứng phó Sự cố và Xử lý Thông tin Trái pháp luật

Nhiệm vụ: Phòng ngừa, xử lý thông tin; Phòng, chống gián điệp mạng; Phòng, chống tấn công mạng.

STT	Nội dung	Căn cứ Pháp lý (Chủ yếu)	Thời gian kế tiếp/Ghi chú	ĐV thực hiện
9.	Xây dựng Phương án Ứng phó Sự cố: Xây dựng phương án cụ thể cho các tình huống như: tuyên truyền chống Nhà nước, gián điệp mạng, tấn công mạng, và khủng bố mạng.	NĐ 53 Điều 25	Xây dựng quy định về an toàn an ninh mạng	Phòng HCQT
10.	Xử lý và Gỡ bỏ Thông tin Vi phạm: Thiết lập quy trình triển khai biện pháp quản lý, kỹ thuật để phòng ngừa, phát hiện, ngăn chặn, gỡ bỏ thông tin có nội dung vi phạm pháp luật (như xuyên tạc, vu khống, thông tin sai sự thật gây hoang mang) trên hệ thống thuộc Trường khi có yêu cầu.	Luật ANM Điều 16;18	Thường xuyên: Cán bộ phụ trách giám sát nội dung của Trường (website, diễn đàn nội bộ).	Trung Tâm TT TV
11.	Phòng ngừa Tấn công mạng: Áp dụng biện pháp kỹ thuật để phòng ngừa, ngăn chặn các hành vi tấn công mạng (như phát tán mã độc gây hại, gây rối loạn, xâm nhập) đối với hệ thống thông tin thuộc phạm vi quản lý của Trường.	Luật ANM Điều 19	Liên tục: Đảm bảo hệ thống tường lửa và các công cụ bảo vệ hoạt động hiệu quả.	Phòng HCQT
12.	Thiết lập cơ chế tự diễn tập và kiểm tra ứng phó: Thực hiện Huấn luyện, diễn tập, phòng ngừa sự cố định kỳ	CV 357 Mục 2; Luật ANM Điều 14; NĐ 53 Điều 25	Thực hiện tự diễn tập mô phỏng và kiểm tra dự phòng định kì 6 tháng	Phòng HCQT

3.4. Nhân lực, Đào tạo và Nâng cao Nhận thức

Nhiệm vụ: Nâng cao nhận thức và đề xuất bổ sung, tăng cường nhân lực.

STT	Nội dung	Căn cứ Pháp lý (Chủ yếu)	Thời gian kế tiếp/Ghi chú	ĐV thực hiện
13.	Rà soát và Đề xuất Tăng cường Nhân lực: Rà soát đánh giá, xác định nhu cầu nhân lực an ninh mạng. Đảm bảo nhân sự có trình độ chuyên môn và cam kết bảo mật thông tin. Đề xuất bổ sung, tăng cường nhân lực cho Trường.	CV 357 Mục 4; NĐ 53 Điều 9	Quý I/2026: Rà soát và lập báo cáo đề xuất nhân sự gửi cấp trên.	Phòng TC& CTHSSV
14.	Triển khai nội dung An ninh mạng vào Tuần sinh hoạt chính trị đầu khóa đảm bảo nội dung giáo dục, bồi dưỡng kiến thức an ninh mạng cho HSSV.	Luật ANM Điều 33		Phòng TC& CTHSSV
15.	Tổ chức Bồi dưỡng, tự bồi dưỡng	Luật	Triển khai kế hoạch	Tất cả

	nghiệp vụ an ninh mạng cho viên chức, người lao động tham gia bảo vệ an ninh mạng tại đơn vị.	ANM Điều 33	an toàn an ninh mạng.	các đơn vị
16.	Tuyên truyền cho Học sinh, Sinh viên: Tiếp tục triển khai công tác tuyên truyền, phổ biến để nâng cao nhận thức của học sinh, sinh viên về nguy cơ an ninh mạng.	CV 357 Mục 3; Luật ANM Điều 34	Tăng cường phổ biến qua các kênh truyền thông của Trường (website, mạng xã hội, thông báo).	Trung Tâm TT TV
17.	Bảo vệ Học sinh - Sinh viên: Kiểm soát nội dung thông tin không gây nguy hại cho Học sinh - Sinh viên và ngăn chặn việc chia sẻ, xóa bỏ thông tin gây nguy hại trên hệ thống dịch vụ của Trường.	Luật ANM Điều 29	Liên tục: Áp dụng chính sách kiểm duyệt nội dung cho các diễn đàn, cổng thông tin nội bộ.	Trung Tâm TT TV

3.5. Tín nhiệm mạng, Lòng tin số và Nguồn Kinh phí

Nhiệm vụ: Tổ chức đánh giá tín nhiệm mạng; củng cố lòng tin số của viên chức, học sinh – sinh viên; Đảm bảo kinh phí.

STT	Nội dung	Căn cứ Pháp lý (Chủ yếu)	Thời gian kế tiếp/Ghi chú	ĐV thực hiện
18.	Tổ chức Đánh giá Tín nhiệm mạng: Chủ động đề nghị Lực lượng chuyên trách bảo vệ an ninh mạng (thuộc Bộ Công an hoặc cơ quan chuyên môn cấp tỉnh) tiến hành kiểm tra an ninh mạng đối với website chính thức (là một dạng Trang thông tin điện tử) và các hệ thống dịch vụ quan trọng khác (nếu có), nhằm phát hiện lỗ hổng và rủi ro bảo mật.	CV 357 Mục 5; Luật ANM Điều 24; 26	Lấy kết quả kiểm tra/rà soát từ cơ quan chuyên trách làm cơ sở để đánh giá mức độ an toàn của hệ thống và công khai các biện pháp khắc phục nhằm củng cố lòng tin số của người dân. Thời gian: Quý II/2026.	Phòng HCQT
19.	Củng cố Lòng tin số: Đảm bảo các hoạt động bảo mật nhằm mục tiêu củng cố lòng tin số của người dân (sinh viên, phụ huynh) khi họ hoạt động, tương tác, làm việc trên không gian mạng với Trường.	CV 357 Mục 5	Liên tục: Duy trì ổn định và an toàn các dịch vụ công trực tuyến.	Phòng HCQT
20.	Quản lý và Bố trí Kinh phí an ninh mạng: Lập dự toán, quản lý, sử dụng và quyết toán kinh phí bảo vệ an ninh mạng và đảm bảo kinh phí được bố trí trong dự toán ngân sách nhà nước hằng năm.	Luật ANM Điều 35; NĐ 53 Điều 28	Đảm bảo kinh phí được ưu tiên và bố trí đầy đủ.	KH-TC
21.	Phối hợp với Lực lượng Chuyên trách:	Luật ANM	Thường xuyên/Đột	Phòng

	Kịp thời cung cấp thông tin liên quan đến nguy cơ đe dọa an ninh mạng và hành vi xâm phạm an ninh mạng cho cơ quan có thẩm quyền.	Điều 24; 42	xuất: Thiết lập đầu mối liên lạc (contact point) với Lực lượng chuyên trách thuộc Bộ Công an.	HCQT

Trên đây là Kế hoạch Tăng cường đảm bảo an ninh mạng, bảo mật thông tin, an toàn dữ liệu của Trường Cao đẳng Sơn La, yêu cầu viên chức, người lao động, học sinh sinh viên nghiêm túc triển khai, thực hiện./.

Nơi nhận:
- Ban Giám hiệu *(Chỉ đạo);*
- Các đơn vị trực thuộc *(Thực hiện)*;
- Lưu: VT, HCQT.

KT. HIỆU TRƯỞNG
PHÓ HIỆU TRƯỞNG

TRƯỜNG CAO ĐẲNG SƠN LA

Nguyễn Xuân Thắng