UBND TỈNH ĐẮK LẮK
SỞ GIÁO DỤC VÀ ĐÀO TẠO

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

QUY CHẾ
Bảo đảm an toàn thông tin, an ninh mạng trong hoạt động ứng dụng công nghệ thông tin của Sở GDĐT

(Kèm theo Quyết định số 946/QĐ-SGDĐT ngày 03 /11/2025 của Sở GDĐT)

Chương I
QUY ĐỊNH CHUNG

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

1. Quy chế này quy định về đảm bảo An toàn thông tin, an ninh mạng trong các hoạt động ứng dụng công nghệ thông tin của Sở Giáo dục và Đào tạo (GDĐT) và các hệ thống thông tin dùng chung ngành GDĐT tỉnh Đắk Lắk.

2. Quy chế này áp dụng đối với:

a) Cán bộ quản lý, công chức và người lao động thuộc Sở GDĐT. Cán bộ quản lý, viên chức và người lao động trong toàn ngành thuộc các đơn vị sự nghiệp giáo dục.

b) Cơ quan, đơn vị, cá nhân có sử dụng hoặc kết nối truy cập vào hệ thống mạng của Sở GDĐT, các hệ thống thông tin thuộc ngành GDĐT tỉnh Đắk Lắk.

c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ quản lý, vận hành, bảo trì, phát triển và đảm bảo an toàn thông tin mạng cho Sở GDĐT.

Điều 2. Giải thích từ ngữ

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

1. *Hệ thống mạng:* bao gồm dịch vụ kết nối Internet; mạng nội bộ; mạng truyền số liệu chuyên dùng.

2. *Hệ thống máy chủ* là một tập hợp các máy tính và các thành phần liên quan được sử dụng để cung cấp các dịch vụ và tài nguyên cho các thiết bị và người dùng trong mạng, được thiết kế để xử lý, lưu trữ, quản lý và chia sẻ thông tin, ứng dụng và dịch vụ.

3. *Trung tâm dữ liệu* là cơ sở hạ tầng tích hợp được thiết kế để lưu trữ, quản lý và xử lý dữ liệu. Trung tâm bao gồm các thành phần chính như máy chủ, thiết bị lưu trữ, thiết bị mạng, hệ thống làm mát, nguồn điện dự phòng và các biện pháp bảo mật vật lý, đảm bảo hoạt động ổn định, an toàn và liên tục của các ứng dụng, dịch vụ công nghệ thông tin. Trung tâm dữ liệu đóng vai trò cốt lõi trong việc hỗ trợ các cơ quan, đơn vị triển khai và vận hành các hệ thống thông tin chuyên ngành, ứng dụng trực tuyến và lưu trữ dữ liệu.

4. *Tường lửa* là rào chắn (phần cứng, phần mềm) được lập ra nhằm kiểm soát người dùng mạng Internet truy nhập vào các thông tin không mong muốn và

người dùng từ bên ngoài truy nhập trái phép thông tin trong mạng nội bộ.

5. *Giám sát an ninh mạng* là hoạt động thu thập, phân tích tình hình nhằm xác định nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật, mã độc, phần cứng độc hại để cảnh báo, khắc phục, xử lý.

6. *TCVN 11930:2017* là tiêu chuẩn quốc gia về công nghệ thông tin - các kỹ thuật an toàn - yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

7. *Tấn công DDoS (Distributed Denial of Service)* là hình thức xâm nhập trái phép hệ thống website và máy chủ của doanh nghiệp. Đây là phương thức tấn công mạng rất phổ biến, được các hacker thường xuyên sử dụng.

8. *Mạng ngang hàng* là mô hình mạng mà trong đó các máy tính có quyền bình đẳng như nhau, mỗi máy tính có quyền chia sẻ tài nguyên và sử dụng các tài nguyên từ máy tính khác.

9. *Mạng nội bộ (LAN - Local Area Network)* là một hệ thống mạng nội bộ được thiết kế để kết nối các thiết bị mạng trong một phạm vi nhỏ với nhau, chẳng hạn như hệ thống mạng trong một văn phòng, trường học hoặc tòa nhà....Mạng nội bộ bao gồm mạng nội bộ có dây và mạng nội bộ không dây (Wifi).

10. *Mạng WAN ((Wide Area Network)* là mạng diện rộng vì không chỉ nằm trong phạm vi một tòa nhà hoặc khuôn viên rộng lớn mà còn mở rộng ra nhiều vị trí trải dài trên một khu vực địa lý cụ thể, hoặc thậm chí trên khắp thế giới.

11. *SAN (Storage Area Network)* là một hệ thống lưu trữ dữ chuyên dụng cho việc kết nối các thiết bị lưu trữ như ổ cứng, đĩa quang, băng từ với các máy chủ.

12. *NAS (Network Attached Storage)* là một thiết bị lưu trữ kết nối với mạng, cho phép nhiều người dùng truy cập và chia sẻ dữ liệu từ xa. Khác với các giải pháp lưu trữ truyền thống như ổ cứng ngoài hay USB, NAS hoạt động như một máy chủ lưu trữ độc lập, cho phép người dùng truy cập dữ liệu thông qua mạng nội bộ hoặc Internet, giúp việc chia sẻ dữ liệu giữa các thiết bị và người dùng trở nên đơn giản, an toàn và hiệu quả.

13. *An toàn thông tin mạng:* là sự bảo vệ thông tin số và các 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.

14. *Trang thiết bị công nghệ thông tin cá nhân:* bao gồm máy tính để bàn, máy tính xách tay, thiết bị số (máy tính bảng, điện thoại thông minh) của cá nhân

Điều 3. Phạm vi đảm bảo an toàn thông tin, an ninh mạng

1. Hệ thống mạng.

2. Hệ thống thông tin quản lý, gồm: các phần mềm nghiệp vụ và cơ sở dữ liệu phục vụ công tác quản lý, điều hành hoạt động của Sở, ngành GDĐT.

3. Trang thiết bị công nghệ thông tin cá nhân**.**

Điều 4. Nguyên tắc chung bảo đảm an toàn thông tin và an ninh mạng

1. Đảm bảo an toàn thông tin mạng là yêu cầu bắt buộc, thường xuyên, liên

tục, có tính xuyên suốt quá trình, đồng bộ từ khi thiết kế, xây dựng, vận hành, nâng cấp và hủy bỏ hệ thống thông tin. Đảm bảo an toàn thông tin mạng phải tuân thủ các nguyên tắc chung, được quy định tại Điều 4 Luật An toàn thông tin mạng và Điều 4 Nghị định số 85/2016/NĐ-CP ngày 01/07/ 2016 của Chính phủ.

2. Việc vận hành hệ thống thông tin đảm bảo các yêu cầu về an toàn thông tin mạng và sẵn sàng xử lý sự cố an toàn thông tin mạng đối với các hệ thống thông tin; bố trí nhân sự chuyên trách chịu trách nhiệm bảo đảm an toàn, an ninh thông tin mạng.

3. Xác định rõ quyền hạn, trách nhiệm của lãnh đạo đơn vị, lãnh đạo phòng chuyên môn nghiệp vụ, từng bộ phận, cá nhân trong Sở GDĐT, các đơn vị có liên quan đối với công tác bảo đảm an toàn thông tin, an ninh mạng trong phạm vi xử lý công việc của mình theo quy định của Nhà nước và của Sở GDĐT.

4. Thông tin mật, thông tin thuộc Danh mục bí mật nhà nước phải được bảo vệ theo quy định của Nhà nước và các quy định khác về công tác bảo vệ bí mật nhà nước và các nội dung tương ứng trong Quy chế này.

5. Xử lý sự cố an toàn thông tin mạng phải phù hợp với trách nhiệm, quyền hạn và đảm bảo lợi ích hợp pháp của cơ quan, đơn vị, cá nhân liên quan và theo

Điều 5. Các hành vi bị nghiêm cấm

1. Các hành vi bị nghiêm cấm về an toàn, an ninh thông tin mạng quy định tại Điều 7 Luật An toàn thông tin mạng, Điều 8 Luật An ninh mạng, Điều 5 Luật Bảo vệ bí mật nhà nước ngày 15 tháng 11 năm 2018.

2. Các hành vi bị cấm trong quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng quy định tại Điều 8 Luật An ninh mạng, Điều 9 Luật Viễn thông ngày 24 tháng 11 năm 2023, quyền và nghĩa vụ của người sử dụng Internet theo quy định tại Điều 7 Nghị định số 147/2024/NĐ-CP ngày 09 tháng 11 năm 2024 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng.

3. Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập mạng không dây của cá nhân vào mạng nội bộ; tự ý thay đổi các cài đặt hệ thống mạng của cơ quan, đơn vị.

4. Tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên thiết bị CNTT phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc.

5. Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin; ngăn chặn việc truy nhập đến thông tin của cơ quan, đơn vị và cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

6. Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, đơn vị và cá nhân khác trên môi trường mạng.

7. Các hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, đơn vị và cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

Chương II

QUY ĐỊNH BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Điều 6. Bảo vệ bí mật Nhà nước trong hoạt động ứng dụng công nghệ thông tin

1. Quy định về soạn thảo, in ấn, phát hành và sao chụp tài liệu mật

a) Không được sử dụng máy tính hoặc các thiết bị khác đã kết nối hoặc đang kết nối với mạng Internet, mạng máy tính, mạng viễn thông, trừ trường hợp lưu trữ bí mật nhà nước theo quy định của pháp luật về cơ yếu để soạn thảo, chuyển giao, lưu trữ tài liệu có nội dung bí mật Nhà nước; cung cấp tin, tài liệu có nội dung bí mật Nhà nước trên mạng xã hội (Zalo; Telegram; Facebook; ...) và đưa thông tin có nội dung bí mật Nhà nước trên Cổng/Trang thông tin điện tử.

b) Không được in, sao chụp tài liệu có nội dung bí mật Nhà nước trên các thiết bị có kết nối mạng internet, mạng máy tính, mạng viễn thông, trừ trường hợp theo quy định của pháp luật về cơ yếu.

c) Phải bố trí ít nhất 01 máy tính riêng và phải được kiểm tra an ninh, an toàn thông tin, không kết nối mạng Internet, mạng máy tính, mạng viễn thông, trừ trường hợp theo quy định của pháp luật về cơ yếu dùng để quản lý, lưu trữ, soạn thảo các tài liệu có nội dung bí mật Nhà nước.

2. Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo, lưu trữ tài liệu có nội dung bí mật Nhà nước, các phòng chuyên môn phải báo cáo cho người có thẩm quyền cho ý kiến. Không được thuê, hợp đồng, cho phép các tổ chức, cá nhân không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố.

3. Trước khi thanh lý các máy tính trong các cơ quan Nhà nước, cán bộ chuyên trách về công nghệ thông tin phải tháo ổ cứng (thanh lý không kèm ổ cứng hoặc các thiết bị lưu trữ khác gắn kèm) và dùng các biện pháp kỹ thuật chuyên biệt để xoá bỏ vĩnh viễn dữ liệu lưu trữ trong ổ cứng, các thiết bị lưu trữ khác gắn kèm hoặc phá hủy về mặt vật lý ổ cứng, các thiết bị lưu trữ khác nếu chứa các tài liệu có nội dung bí mật Nhà nước.

Điều 7. Quy định về cấp phát, thu hồi, cập nhật và quản lý các tài khoản truy cập vào hệ thống thông tin dùng chung của ngành GDĐT

1. Mỗi cá nhân, đơn vị được cấp các tài khoản truy cập các ứng dụng dùng chung của đơn vị, ngành gắn với cá nhân đó, đơn vị đó và chỉ truy cập vào các Trang/Cổng thông tin điện tử, ứng dụng trực tuyến phù hợp với chức năng, trách nhiệm, quyền hạn của mình. Trường hợp sử dụng tài khoản dùng chung cho một nhóm người hay một đơn vị, phải có cơ chế xác định các cá nhân, đơn vị có trách nhiệm quản lý tài khoản. Người dùng chỉ được truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình và có trách nhiệm bảo mật tài khoản truy cập được cấp.

2. Tài khoản quản trị hệ thống (mạng máy tính, hệ điều hành, thiết bị kết nối mạng, phần mềm ứng dụng, cơ sở dữ liệu, hệ thống thông tin) phải tách biệt với tài khoản truy cập của người sử dụng thông thường. Tài khoản hệ thống phải được giao đích danh cá nhân làm công tác quản trị.

3. Bộ phận, công chức, viên chức được giao quản trị các hệ thống thông tin

cấp, khóa quyền truy cập của tài khoản các hệ thống thông tin trong trường hợp tài khoản đó thực hiện các hành vi tấn công hoặc để xảy ra vấn đề mất an toàn thông tin, an ninh mạng.

4. Trường hợp cán bộ thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu, trong vòng không quá 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 cơ quan, đơn vị, người có thẩm quyền để điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng đối với hệ thống thông tin.

5. Mật mã đăng nhập, truy cập hệ thống thông tin có độ dài tối thiểu 08 ký tự, bao gồm ký tự in hoa, ký tự in thường, ký tự số và ký tự đặc biệt (!, @, #, %, $, *, &).

Điều 8. Quản lý trang thiết bị ứng dụng công nghệ thông tin trong hoạt động của cơ quan, đơn vị

1. Giao, gắn trách nhiệm cho cá nhân hoặc tập thể quản lý, sử dụng trang thiết bị ứng dụng CNTT trong hoạt động cơ quan, đơn vị.

2. Cơ quan, đơn vị quy định các quy tắc sử dụng, giữ gìn bảo vệ trang thiết bị ứng dụng CNTT trong hoạt động cơ quan, đơn vị trong các trường hợp như: mang ra khỏi cơ quan, trang thiết bị ứng dụng CNTT trong hoạt động cơ quan, đơn vị liên quan đến dữ liệu nhạy cảm, cài đặt và cấu hình.

3. Trang thiết bị ứng dụng CNTT trong hoạt động cơ quan, đơn vị khi thay đổi mục đích sử dụng hoặc thanh lý thì cơ quan, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó đảm bảo không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, đơn vị phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên trang thiết bị ứng dụng CNTT trong hoạt động cơ quan, đơn vị đó.

4. Thiết bị tính toán có bộ phận lưu trữ hoặc thiết bị lưu trữ khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài hoặc ngừng sử dụng phải tháo bộ phận lưu trữ khỏi thiết bị hoặc xóa thông tin, dữ liệu lưu trữ trên thiết bị (trừ trường hợp để khôi phục dữ liệu).

5. Cơ quan, đơn vị có trách nhiệm xây dựng quy trình bảo dưỡng, bảo trì và hướng dẫn cách sử dụng, quản lý, vận hành hệ thống hạ tầng kỹ thuật của đơn vị; thực hiện quản lý, vận hành và định kỳ kiểm tra, sửa chữa, bảo trì thiết bị (bao gồm thiết bị dự phòng).

Điều 9. Quản lý cán bộ, công chức, viên chức và người lao động

1. Cơ quan, đơn vị tổ chức quán triệt các quy định về an toàn thông tin nhằm nâng cao nhận thức về trách nhiệm bảo đảm an toàn, an ninh thông tin của từng cá nhân trong cơ quan, đơn vị.

2. Cán bộ, công chức, viên chức, người lao động phải tuân thủ thực hiện các quy định bảo đảm an toàn, an ninh thông tin của cơ quan, đơn vị.

3. Cần phải bố trí nhân sự có năng lực và đạo đức đảm nhận vị trí phụ trách công tác bảo đảm an toàn, an ninh thông tin, quản trị hệ thống CNTT của cơ quan, đơn vị.

4. Cơ quan, đơn vị lập kế hoạch đào tạo cho cán bộ, công chức, viên chức và người lao động để nâng cao kiến thức cơ bản và kỹ năng an toàn mạng, an toàn, an ninh thông tin; đồng thời, phổ biến, cập nhật các quy chế về an toàn, an ninh thông tin hằng năm để mọi người hiểu rõ các quyền và trách nhiệm đối với việc bảo đảm an toàn thông tin. Kiểm tra việc thực hiện các nội quy, quy định về an toàn, an ninh thông tin của cơ quan, đơn vị đối với cán bộ, công chức, viên chức, người lao động theo định kỳ.

5. Khi chấm dứt hoặc thay đổi công việc, cơ quan, đơn vị phải: Xác định rõ trách nhiệm của cán bộ, công chức, viên chức, người lao động và các bên liên quan về hệ thống CNTT; hủy tài khoản, quyền truy cập hoặc thay đổi quyền truy cập hệ thống CNTT (như: *mật khẩu, chứng thư số, thư mục lưu trữ, thư điện tử, máy vi tính, thiết bị lưu trữ dùng chung, ...*) phù hợp với công việc được thay đổi.

Điều 10. Bảo đảm an toàn hệ thống công nghệ thông tin

1. Bảo đảm an toàn thông tin khi sử dụng máy tính

a) Cá nhân chỉ cài đặt phần mềm hợp lệ (phần mềm có bản quyền thương mại, phần mềm nội bộ được đầu tư hoặc phần mềm mã nguồn mở có nguồn gốc rõ ràng) và thuộc danh mục phần mềm được phép sử dụng do cơ quan có thẩm quyền ban hành (nếu có) trên máy tính được đơn vị cấp; 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.

b) Cá nhân cài đặt phần mềm phòng, chống mã độc có bản quyền 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.

c) Cá nhân chỉ truy nhập 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 nhập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác.

2. Bảo đảm an toàn thông tin đối với hệ thống mạng máy tính của cơ quan, đơn vị

a) Hệ thống mạng nội bộ (LAN) phải được thiết kế phân vùng theo chức năng cơ bản phù hợp chính sách an toàn thông tin riêng của cơ quan, đơn vị, bao gồm: vùng mạng người dùng; vùng mạng kết nối hệ thống ra bên ngoài Internet và các mạng khác; vùng mạng máy chủ công cộng; vùng mạng máy chủ nội bộ; vùng mạng máy chủ quản trị. Dữ liệu trao đổi giữa các vùng mạng phải được quản lý, giám sát bởi hệ thống các thiết bị mạng, thiết bị bảo mật.

b) Định kỳ sao lưu thông tin, dữ liệu dùng chung lưu trữ trên mạng diện rộng; không được tiết lộ phương thức đăng nhập (các thông tin như; tên đăng ký, mật khẩu, tiện ích, tệp hỗ trợ và các cách thức khác) cho các tổ chức, cá nhân khác để truy nhập vào hệ thống mạng diện rộng; không được tìm cách truy nhập dưới bất cứ hình thức nào vào các khu vực không được phép truy nhập.

c) Áp dụng các biện pháp kỹ thuật cần thiết bảo đảm an toàn thông tin trong hoạt động kết nối internet, tối thiểu đáp ứng các yêu cầu sau: có hệ thống tường lửa và hệ thống bảo vệ truy nhập Internet, đáp ứng nhu cầu kết nối, đồng thời, hỗ trợ các công nghệ mạng riêng ảo thông dụng và có phần cứng mã hóa tích hợp để tăng tốc độ mã hóa dữ liệu và có khả năng bảo vệ hệ thống trước các loại tấn công từ chối dịch vụ (DDoS); lọc bỏ, không cho phép truy nhập các trang tin có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp.

d) Các đường truyền dữ liệu, đường truyền Internet và các hệ thống dây dẫn các mạng LAN, WAN phải được lắp đặt trong ống, máng che đậy kín, hạn chế khả năng tiếp cận trái phép. Ngắt kết nối cổng Ethernet không sử dụng, đặc biệt là ở khu vực làm việc chung của các cơ quan, đơn vị.

3. Quản lý tài khoản truy cập

a) Cá nhân sử dụng hệ thống thông tin được cấp và sử dụng tài khoản truy nhập với định danh duy nhất gắn với cá nhân đó.

b) Chủ tài khoản không chia sẻ, giao quyền tài khoản và mật khẩu truy nhập cho người khác. Không sử dụng tài khoản của người khác để đăng nhập vào hệ thống thông tin, cơ sở dữ liệu.

c) Tài khoản thư điện tử ngành GDĐT theo tên miền ***gddt.daklak.gov.vn*** hoặc ***daklak.edu.vn*** để phục vụ cho các hoạt động mang tính nghiệp vụ ngành, không sử dụng để giao dịch, đăng ký trên mạng xã hội, các trang thông tin điện tử công cộng khác; định kỳ 01 năm kiểm tra việc lưu trữ của hệ thống thư điện tử, tiến hành xóa các email quá cũ, không cần thiết để bảo đảm hệ thống hoạt động ổn định thông suốt.

d) Tài khoản quản trị hệ thống được giao cho cán bộ chuyên trách về công nghệ thông tin phục vụ cho công tác quản trị, phân quyền, cấu hình hệ thống đó.

đ) Cán bộ quản trị hệ thống không sử dụng cùng một mật khẩu cho nhiều tài khoản khác nhau.

e) Trường hợp cá nhân thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu, trong vòng không quá 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 cơ quan, đơn vị vận hành hệ thống thông tin bằng văn bản có xác nhận của thủ trưởng đơn vị để điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng đối với hệ thống thông tin.

g) Tài khoản quản trị hệ thống (như: 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 nhập của người sử dụng thông thường. Tài khoản hệ thống phải được giao đích danh cá nhân làm công tác quản trị. Hạn chế dùng chung tài khoản quản trị.

h) Khi có yêu cầu khóa quyền truy cập hệ thống thông tin của tài khoản đang hoạt động, lãnh đạo đơn vị phải yêu cầu bằng văn bản gửi đơn vị chủ quản hệ thống thông tin hoặc đơn vị được giao vận hành trực tiếp hệ thống thông tin để xem xét, thực hiện. Đơn vị vận hành hệ thống thông tin 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.

4. Bảo đảm an toàn thông tin mức ứng dụng

a) Yêu cầu về bảo đảm an toàn thông tin phải được đưa vào tất cả các công đoạn thiết kế, xây dựng, triển khai và vận hành, sử dụng phần mềm, ứng dụng.

b) Phần mềm, ứng dụng phải đáp ứng các yêu cầu sau: cấu hình phần mềm, ứng dụng để xác thực người sử dụng; giới hạn số lần đăng nhập sai liên tiếp; giới hạn thời gian để chờ đóng phiên kết nối; mã hóa thông tin xác thực trên hệ thống; không khuyến khích việc đăng nhập tự động.

c) Thiết lập, phân quyền truy nhập, quản trị, sử dụng tài nguyên khác nhau của phần mềm, ứng dụng với người sử dụng/nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau; tách biệt cổng giao tiếp quản trị phần mềm ứng dụng với cổng giao tiếp cung cấp dịch vụ; đóng các cổng giao tiếp không sử dụng.

d) Chỉ cho phép sử dụng các giao thức mạng có hỗ trợ chức năng mã hóa thông tin như SSH, SSL, VPN hoặc tương đương khi truy nhập, quản trị phần mềm, ứng dụng từ xa trên môi trường mạng; hạn chế truy cập đến mã nguồn của phần mềm, ứng dụng và phải đặt mã nguồn trong môi trường an toàn do bộ phận chuyên trách CNTT quản lý.

đ) Ghi và lưu giữ bản ghi nhật ký hệ thống của phần mềm, ứng dụng trong khoảng thời gian tối thiểu 90 ngày với những thông tin cơ bản: thời gian, địa chỉ, tài khoản (nếu có), nội dung truy nhập và sử dụng phần mềm, ứng dụng; các lỗi phát sinh trong quá trình hoạt động; thông tin đăng nhập khi quản trị.

e) Phần mềm, ứng dụng cần được kiểm tra phát hiện và khắc phục các điểm yếu về an toàn, an ninh thông tin trước khi đưa vào sử dụng và trong quá trình sử dụng.

g) Thực hiện quy trình kiểm soát cài đặt, cập nhật, vá lỗi bảo mật phần mềm, ứng dụng trên các máy chủ, máy tính cá nhân, thiết bị kết nối mạng đang hoạt động thuộc hệ thống mạng nội bộ.

5. Bảo đảm an toàn thông tin mức dữ liệu

a) Cơ quan, đơn vị phải thực hiện bảo vệ thông tin, dữ liệu liên quan đến hoạt động công vụ, thông tin có nội dung quan trọng, nhạy cảm hoặc không phải là thông tin công khai bằng các biện pháp như: thiết lập phương án bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu; mã hóa thông tin, dữ liệu khi lưu trữ trên hệ thống/thiết bị lưu trữ dữ liệu di động; sử dụng chữ ký số để xác thực và bảo mật thông tin, dữ liệu.

b) Cơ quan, đơn vị cần triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

c) Cơ quan, đơn vị cần bố trí máy tính riêng không kết nối mạng, đặt mật khẩu, mã hóa dữ liệu và các biện pháp bảo mật khác bảo đảm an toàn thông tin để soạn thảo, lưu trữ dữ liệu, thông tin và tài liệu quan trọng ở các mức độ mật, tối mật, tuyệt mật.

d) Cơ quan, đơn vị phải thường xuyên kiểm tra, giám sát các hoạt động chia sẻ, gửi, nhận thông tin, dữ liệu trong hoạt động nội bộ của mình; khuyến cáo việc chia sẻ, gửi, nhận thông tin trên môi trường mạng cần phải sử dụng mật khẩu để bảo vệ thông tin.

đ) Đối với hoạt động trao đổi thông tin, dữ liệu với bên ngoài, cơ quan, đơn vị và cá nhân thực hiện trao đổi thông tin, dữ liệu ra bên ngoài cam kết và có biện pháp bảo mật thông tin, dữ liệu được trao đổi. Giao dịch trực tuyến phải được truyền đầy đủ, đúng địa chỉ, tránh bị sửa đổi, tiết lộ hoặc nhân bản một cách trái phép; sử dụng các cơ chế xác thực mạnh, chữ ký số khi tham gia giao dịch, sử dụng các giao thức truyền thông an toàn.

Điều 11. Xác định cấp độ và phương án bảo đảm an toàn hệ thống thông tin

1. Việc xác định cấp độ hệ thống thông tin và xây dựng phương án bảo vệ hệ thống thông tin theo cấp độ phục vụ mục đích đánh giá an toàn thông tin và bảo đảm an toàn thông tin cho các hệ thống thông tin. Nguyên tắc bảo đảm an toàn thông tin theo cấp độ và nguyên tắc xác định cấp độ căn cứ trên các nguyên tắc quy định tại Điều 4, Điều 5 Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ.

2. Đảm bảo an toàn hệ thống thông tin theo cấp độ trong hoạt động của cơ quan, tổ chức phải được thực hiện thường xuyên, liên tục từ khâu thiết kế, xây dựng, vận hành đến khi hủy bỏ; tuân thủ theo tiêu chuẩn, quy chuẩn kỹ thuật. Nội dung yêu cầu bảo đảm an toàn hệ thống thông tin theo cấp độ thực hiện theo quy định tại Điều 9 và Điều 10 Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ.

3. Đánh giá, phân loại cấp độ an toàn thông tin của hệ thống thông tin

a) Chủ quản hệ thống thông tin có trách nhiệm chỉ đạo, tổ chức thực hiện phương án đảm bảo an toàn hệ thống thông tin theo cấp độ theo quy định tại Nghị định số 85/2016/NĐ-CP.

b) Đơn vị vận hành hệ thống thông tin thực hiện xác định cấp độ và lập hồ sơ đề xuất cấp độ bao gồm các tài liệu được quy định tại Điều 15 Nghị định số 85/2016/NĐ-CP, gửi cơ quan có thẩm quyền thẩm định, phê duyệt theo quy định tại khoản 1 Điều 14 Nghị định số 85/2016/NĐ-CP.

4. Hệ thống thông tin khi được đầu tư xây dựng mới hoặc mở rộng, nâng cấp cần được kiểm thử về tính an toàn, bảo mật trước khi nghiệm thu, bàn giao đưa vào khai thác, sử dụng theo quy định tại điểm b khoản 3 Điều 10 Thông tư số

24/2020/TT-BTTTT ngày 09 tháng 9 năm 2020 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về công tác triển khai, giám sát công tác triển khai và nghiệm thu dự án đầu tư ứng dụng CNTT sử dụng nguồn vốn ngân sách nhà nước.

5. Phương án bảo đảm an toàn hệ thống thông tin

a) Phương án bảo đảm an toàn hệ thống thông tin phải phù hợp với cấp độ của hệ thống thông tin và đáp ứng yêu cầu quy định tại Điều 9, Điều 10 Thông tư số 12/2022/TT-BTTTT; phù hợp với Tiêu chuẩn Quốc gia TCVN 11930:2017 Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ; các tiêu chuẩn, quy chuẩn kỹ thuật khác và chính sách an toàn thông tin mạng (nếu có).

b) Chủ quản hệ thống thông tin hoặc đơn vị được ủy quyền quản lý trực tiếp hệ thống thông tin tổ chức triển khai phương án bảo đảm an toàn hệ thống thông tin sau khi hồ sơ đề xuất cấp độ hoặc phương án bảo đảm an toàn hệ thống được phê duyệt.

c) Đơn vị/bộ phận chuyên trách về an toàn thông tin thuộc đơn vị chịu trách nhiệm giám sát việc triển khai các phương án bảo đảm an toàn thông tin đã được phê duyệt.

Điều 12. Giám sát an toàn thông tin mạng

1. Chủ quản hệ thống thông tin chỉ đạo việc giám sát đối với các hệ thống thông tin thuộc phạm vi quản lý, phối hợp với đơn vị chuyên trách về an toàn thông tin của tỉnh và các đơn vị chức năng của Sở Khoa học và Công nghệ giám sát theo quy định.

2. Nguyên tắc, yêu cầu, nội dung, phương thức, hệ thống kỹ thuật phục vụ công tác giám sát thực hiện theo quy định tại Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) quy định hoạt động giám sát an toàn hệ thống thông tin.

3. Đơn vị chuyên trách về an toàn thông tin của cơ quan, đơn vị cử 01 lãnh đạo đơn vị và 01 cán bộ (hoặc 01 đơn vị trực thuộc) làm đầu mối giám sát an toàn thông tin mạng để tiếp nhận cảnh báo, cung cấp, trao đổi, chia sẻ thông tin với đơn vị chuyên trách về an toàn thông tin của tỉnh trong các hoạt động giám sát an toàn thông tin tại cơ quan, đơn vị.

Điều 13. Kiểm tra, đánh giá an toàn thông tin mạng

1. Chủ quản hệ thống thông tin có thẩm quyền yêu cầu kiểm tra, đánh giá đối với các hệ thống thông tin thuộc thẩm quyền quản lý. Đơn vị/bộ phận chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin có thẩm quyền yêu cầu kiểm tra, đánh giá đối với các hệ thống thông tin do mình phê duyệt hồ sơ đề xuất cấp độ.

2. Đơn vị chủ trì kiểm tra, đánh giá là đơn vị được cấp có thẩm quyền giao nhiệm vụ hoặc được lựa chọn để thực hiện việc kiểm tra, đánh giá. Đối tượng

kiểm tra, đánh giá là chủ quản hệ thống thông tin hoặc đơn vị vận hành hệ thống thông tin và các hệ thống thông tin có liên quan.

3. Nội dung, hình thức kiểm tra, đánh giá theo quy định tại Điều 11 Thông tư số 12/2022/TT-BTTTT.

4. Đơn vị chuyên trách về an toàn thông tin của tỉnh thực hiện việc kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ tại Tỉnh theo quy định tại Điều 12 Thông tư số 12/2022/TT-BTTTT.

5. Đơn vị chuyên trách về an toàn thông tin của tỉnh, đơn vị chuyên trách về an toàn thông tin của cơ quan, đơn vị thực hiện việc đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin theo thẩm quyền. Nội dung đánh giá là cơ sở để điều chỉnh phương án bảo đảm an toàn thông tin cho phù hợp.

Điều 14. Ứng phó sự cố an toàn thông tin mạng

1. Nguyên tắc ứng cứu xử lý sự cố

a) Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả.

b) Phối hợp chặt chẽ, tuân thủ quy định của pháp luật về điều phối ứng cứu sự cố an toàn thông tin.

c) Ứng cứu xử lý sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin.

d) Việc xử lý sự cố an toàn thông tin phải bảo đảm quyền và lợi ích hợp pháp của cơ quan, đơn vị, cá nhân và bảo mật thông tin cá nhân, thông tin riêng của cơ quan, đơn vị khi tham gia các hoạt động ứng cứu xử lý sự cố.

2. Phân nhóm sự cố an toàn thông tin

a) Sự cố do bị tấn công mạng: tấn công từ chối dịch vụ; tấn công giả mạo; tấn công sử dụng mã độc; truy cập trái phép, chiếm quyền điều khiển; tấn công thay đổi giao diện; tấn công mã hóa phần mềm, dữ liệu, thiết bị; phá hoại thông tin, dữ liệu, phần mềm; nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu; các hình thức tấn công mạng khác.

b) Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật.

c) Sự cố do lỗi của người quản trị, vận hành hệ thống.

d) Sự cố liên quan đến các thảm họa tự nhiên như: bão, lụt, động đất, hỏa hoạn; huy động các nguồn lực nằm ngoài phạm vi của đơn vị vận hành hệ thống thông tin để ứng phó với các sự cố quy định tại khoản 1 điều này theo phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu hoạt động ứng cứu sự cố an toàn thông tin mạng.

3. Phân loại mức độ nghiêm trọng sự cố

a) Thấp: Sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan, đơn vị.

b) Trung bình: Sự cố ảnh hưởng đến một nhóm người dùng nhưng không

gây gián đoạn hay đình trệ hoạt động chính của cơ quan, đơn vị.

c) Cao: Sự cố tác động đến khả năng vận hành của hệ thống thông tin, ảnh hưởng đến dữ liệu, thiết bị, gây ảnh hưởng đến hoạt động chung của cơ quan, đơn vị và hoạt động cung cấp dịch vụ công cho người dân, doanh nghiệp.

d) Nghiêm trọng: Sự cố gây gián đoạn hoặc đình trệ hệ thống trong một khoảng thời gian ngắn, ảnh hưởng nghiêm trọng đến dữ liệu, thiết bị của hệ thống, gây thiệt hại nghiêm trọng cho cơ quan, đơn vị và người dân, doanh nghiệp.

4. Quy trình phối hợp ứng cứu xử lý sự cố

a) Bước 1: Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc thẩm quyền cơ quan, đơn vị trực tiếp quản lý thì thực hiện tiếp; Bước 2. Nếu hệ thống có nguy cơ mất an toàn thông tin mạng thuộc Trung tâm Công nghệ thông tin và Truyền thông trực thuộc Sở Khoa học và Công nghệ quản lý (các hệ thống được triển khai tập trung tại Trung tâm Dữ liệu tỉnh) thì thực hiện tiếp Bước 3.

b) Bước 2: Tiến hành xử lý sự cố theo quy chế nội bộ của cơ quan, đơn vị. Nếu sự cố được khắc phục thì lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố. Khi sự cố vượt quá khả năng xử lý của cơ quan, đơn vị, lập biên bản ghi nhận và thực hiện tiếp Bước 3.

c) Bước 3: Báo sự cố đến Sở Khoa học và Công nghệ hoặc Tiểu ban An toàn, An ninh mạng tỉnh Đắk Lắk.

d) Bước 4: Phối hợp với Sở Khoa học và Công nghệ; Tiểu ban An toàn, An ninh mạng tỉnh Đắk Lắk và các cơ quan, đơn vị, tổ chức có liên quan để tiến hành khắc phục sự cố và thực hiện tiếp Bước 5.

đ) Bước 5: Lập biên bản ghi nhận và kết thúc quy trình phối hợp xử lý sự cố. Lãnh đạo cơ quan, đơn vị phải chỉ đạo kịp thời để khắc phục và hạn chế thiệt hại, báo cáo bằng văn bản cho cơ quan cấp trên trực tiếp quản lý; Sở Khoa học và Công nghệ và Tiểu ban An toàn, An ninh mạng tỉnh Đắk Lắk.

5. Trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của cơ quan, đơn vị, lãnh đạo cơ quan, đơn vị phải báo cáo ngay cho cơ quan cấp trên quản lý trực tiếp và Sở Khoa học và Công nghệ hoặc Tiểu ban An toàn, An ninh mạng tỉnh Đắk Lắk để được hướng dẫn, hỗ trợ.

6. Đơn vị/bộ phận chuyên trách về an toàn thông tin có trách nhiệm.

a) Xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng.

b) Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định.

c) Phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin; yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống.

d) Tổ chức diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo

của lãnh đạo.

Điều 15. Bảo vệ dữ liệu cá nhân trong hệ thống thông tin

1. Đơn vị tham gia sử dụng hệ thống thông tin xử lý dữ liệu cá nhân có trách nhiệm xác định chính xác các cá nhân được phép truy cập hệ thống thông tin để xử lý dữ liệu cá nhân; gửi đề nghị thay đổi, thu hồi tài khoản truy cập hệ thống thông tin tới đơn vị vận hành hệ thống thông tin ngay sau khi có sự thay đổi phân công về xử lý dữ liệu cá nhân tại đơn vị.

2. Cá nhân được cấp tài khoản truy cập hệ thống thông tin để xử lý dữ liệu cá nhân trên hệ thống có trách nhiệm:

a) Giữ bí mật mật khẩu và bảo vệ các phương tiện xác thực khác (nếu có) để truy cập hệ thống thông tin.

b) Không thực hiện các hoạt động xử lý hoặc khai thác dữ liệu cá nhân trên hệ thống thông tin ngoài phạm vi trách nhiệm, nhiệm vụ được phân công.

c) Khi không còn được phân công xử lý dữ liệu cá nhân trên hệ thống thông tin, yêu cầu đơn vị quản lý thực hiện thay đổi, thu hồi tài khoản; có trách nhiệm bàn giao tài khoản cho người tiếp nhận công việc này theo phân công của đơn vị quản lý.

Điều 16. Đào tạo, bồi dưỡng nghiệp vụ, tuyên truyền, phổ biến nâng cao nhận thức về an toàn thông tin mạng

1. Cơ quan, đơn vị xác định nhu cầu về đào tạo nguồn nhân lực bảo đảm an toàn thông tin tại đơn vị, rà soát và đề xuất gửi Sở GDĐT. Sở GDĐT tổng hợp, phối hợp với Sở Khoa học và Công nghệ; Tiểu ban An toàn, An ninh mạng tỉnh Đắk Lắk xây dựng kế hoạch hằng năm về đào tạo, bồi dưỡng nghiệp vụ an toàn, an ninh thông tin cho cán bộ, công chức, viên chức và người lao động trên địa bàn tỉnh và thực hiện tổ chức đào tạo theo kế hoạch đã phê duyệt.

2. Cơ quan, đơn vị tổ chức bồi dưỡng nghiệp vụ về an toàn thông tin cho cán bộ CNTT, cán bộ chuyên trách/kiêm nhiệm về an toàn thông tin mạng của cơ quan, đơn vị; đào tạo cơ bản về an toàn thông tin cho cán bộ quản lý, người sử dụng máy tính thuộc cơ quan, đơn vị.

3. Cơ quan, đơn vị thường xuyên tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức về bảo đảm an toàn thông tin mạng và an ninh mạng đến toàn thể bộ cán bộ, công chức, viên chức và người lao động tại cơ quan, đơn vị.

4. Sở GDĐT tổ chức tuyên truyền, phổ biến nâng cao nhận thức về an toàn thông tin mạng và an ninh mạng đối với ngành giáo dục trên địa bàn tỉnh và thực hiện các nội dung theo kế hoạch đã được phê duyệt.

Chương III
QUY ĐỊNH BẢO ĐẢM AN NINH MẠNG

Điều 17. Triển khai hoạt động bảo vệ an ninh mạng trong cơ quan, đơn vị

1. Nội dung triển khai hoạt động bảo vệ an ninh mạng bao gồm:

a) Xây dựng phương án bảo đảm an ninh mạng đối với hệ thống thông tin; phương án ứng phó, khắc phục sự cố an ninh mạng.

b) Ứng dụng, triển khai phương án, biện pháp, công nghệ bảo vệ an ninh mạng đối với hệ thống thông tin và thông tin, tài liệu được lưu trữ, soạn thảo, truyền đưa trên hệ thống thông tin thuộc phạm vi quản lý.

c) Tổ chức bồi dưỡng kiến thức về an ninh mạng cho cán bộ, công chức, viên chức, người lao động; nâng cao năng lực bảo vệ an ninh mạng cho lực lượng bảo vệ an ninh mạng.

d) Bảo vệ an ninh mạng trong hoạt động cung cấp dịch vụ trực tuyến, cung cấp, trao đổi, thu thập thông tin với cơ quan, tổ chức, cá nhân, chia sẻ thông tin trong nội bộ và với cơ quan khác.

đ) Triển khai kiểm tra an ninh mạng đối với hệ thống thông tin; phòng, chống hành vi vi phạm pháp luật về an ninh mạng; ứng phó, khắc phục sự cố an ninh mạng.

2. Người đứng đầu cơ quan, đơn vị có trách nhiệm triển khai hoạt động bảo vệ an ninh mạng thuộc quyền quản lý.

Điều 18. Bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia

Cơ quan, đơn vị có hệ thống thông tin quan trọng về an ninh quốc gia có trách nhiệm:

1. Kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; thông báo kết quả kiểm tra bằng văn bản trước tháng 10 hằng năm cho lực lượng chuyên trách bảo vệ an ninh mạng theo quy định tại Luật An ninh mạng.

2. Phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng tiến hành kiểm tra an ninh mạng đột xuất.

3. Chủ trì, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền thường xuyên thực hiện giám sát an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý.

4. Xây dựng cơ chế tự cảnh báo và tiếp nhận cảnh báo về nguy cơ đe dọa an ninh mạng, sự cố an ninh mạng, điểm yếu, lỗ hổng bảo mật, mã độc, phần cứng, phần mềm độc hại và đề ra phương án ứng phó, khắc phục khẩn cấp.

5. Xây dựng phương án ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý; triển khai phương án ứng phó, khắc phục khi sự cố an ninh mạng xảy ra và kịp thời báo cáo với lực lượng chuyên trách bảo vệ an ninh mạng có thẩm quyền.

6. Tuân thủ các quy định liên quan khác tại Luật An ninh mạng.

Chương III
TRÁCH NHIỆM BẢO ĐẢM AN TOÀN THÔNG TIN, AN NINH MẠNG VÀ TỔ CHỨC THỰC HIỆN

Điều 19. Trách nhiệm của Sở GDĐT

1. Hướng dẫn triển khai, giám sát, đôn đốc, kiểm tra việc triển khai thực hiện các nội dung tại Quy chế này.

2. Phối hợp với Sở Khoa học và Công nghệ; Tiểu ban An toàn thông tin an ninh mạng tỉnh Đắk Lắk tham mưu giúp Ủy ban nhân dân tỉnh về công tác bảo đảm an toàn thông tin, an ninh mạng trên địa bàn tỉnh.

3. Phối hợp với Công an tỉnh trong việc hướng dẫn, hỗ trợ các đơn vị về công tác bảo đảm an toàn thông tin và an ninh mạng; xây dựng kế hoạch, báo cáo về an toàn thông tin, an ninh mạng của ngành giáo dục và đào tạo.

4. Hằng năm, xây dựng và triển khai các Kế hoạch đào tạo, tập huấn về công tác bảo đảm an toàn thông tin, an ninh mạng cho cán bộ, công chức, viên chức của các cơ quan, đơn vị thuộc phạm vi quản lý. Tổ chức hội nghị, hội thảo chuyên đề và tuyên truyền về an toàn thông tin, an ninh mạng trong công tác quản lý nhà nước của ngành giáo dục và đào tạo trên địa bàn tỉnh.

Điều 20. Trách nhiệm các cơ quan, đơn vị

1. Thủ trưởng cơ quan, đơn vị có trách nhiệm tổ chức thực hiện các quy định tại Quy chế này; chịu trách nhiệm trước pháp luật và Sở GDĐT trong công tác bảo đảm an toàn thông tin, an ninh mạng của cơ quan, đơn vị.

2. Phân công bộ phận hoặc công chức, viên chức chuyên trách/kiêm nhiệm bảo đảm an toàn thông tin, an ninh mạng của cơ quan, đơn vị; chỉ đạo công chức, viên chức và người lao động nghiêm túc chấp hành các quy định về bảo đảm an toàn hông tin, an ninh mạng; tạo điều kiện để các công chức, viên chức phụ trách an toàn thông tin được học tập, nâng cao trình độ về an toàn thông tin, an ninh mạng; thường xuyên tổ chức quán triệt các quy định về an toàn thông tin, an ninh mạng trong cơ quan, đơn vị; xác định các yêu cầu, trách nhiệm bảo đảm an toàn thông tin đối với các vị trí cần tuyển dụng hoặc phân công.

3. Ban hành quy định, quy trình nội bộ về bảo đảm an toàn thông tin gồm các nội dung cơ bản như quy định về quản lý hạ tầng mạng, bảo đảm an toàn dữ liệu, bảo đảm an toàn thiết bị và người dùng đầu cuối phù hợp với Quy chế này và các quy định của pháp luật.

4. Các cơ quan, đơn vị có trách nhiệm thực hiện xác định cấp độ an toàn thông tin và bảo đảm an toàn cho hệ thống thông tin của đơn vị quản lý theo quy định tại Luật An toàn thông tin mạng, Nghị định 85/2016/NĐ-CP và hướng dẫn tại Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về việc bảo đảm an toàn hệ thống thông tin theo cấp độ.

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

6. Phối hợp chặt chẽ với Công an tỉnh, Sở Khoa học và Công nghệ và các cơ quan, đơn vị liên quan trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin.

Điều 21. Trách nhiệm nhiệm cá nhân

1. Thủ trưởng đơn vị thuộc đối tượng áp dụng của Quy chế này có trách nhiệm: phổ biến tới từng cán bộ, công chức, viên chức và người lao động của đơn vị; thường xuyên kiểm tra việc thực hiện Quy chế này tại đơn vị; chịu trách nhiệm trước pháp luật và lãnh đạo cấp trên về các vi phạm, thất thoát thông tin, dữ liệu mật thuộc phạm vị quản lý của đơn vị do không tổ chức, chỉ đạo, kiểm tra cán bộ, công chức, viên chức và người lao động của đơn vị thực hiện theo quy định.

2. Cán bộ, công chức, viên chức và người lao động của các cơ quan, đơn vị thuộc đối tượng áp dụng của quy định có trách nhiệm: Tuân thủ các quy định của Quy chế; thông báo các vấn đề bất thường liên quan tới an toàn thông tin, an ninh mạng cho đơn vị, bộ phận chuyên trách/kiêm nhiệm về an toàn thông tin, an ninh mạng của đơn vị; chịu trách nhiệm trước pháp luật và lãnh đạo đơn vị về các vi phạm, thất thoát dữ liệu mật của đơn vị do không tuân thủ Quy chế.

Điều 22. Tổ chức thực hiện

1. Căn cứ Quy chế này, thủ trưởng các đơn vị có trách nhiệm tổ chức tuyên truyền, phổ biến cho toàn thể cán bộ, công chức, viên chức và người lao động triển khai thực hiện trong phạm vi quản lý.

2. Định kỳ hàng năm hoặc khi có thay đổi chính sách an toàn thông tin thì kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung Quy chế đảm bảo an toàn thông tin, an ninh mạng.

3. Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh các đơn vị phản ánh kịp thời về Sở GDĐT để hướng dẫn thực hiện./.