

TCCS

TIÊU CHUẨN CƠ SỞ

HIỆP HỘI AN TOÀN THÔNG TIN VIỆT NAM



TCCS 03:2024/VNISA

Xuất bản lần 01

**YÊU CẦU KỸ THUẬT CƠ BẢN ĐỐI VỚI SẢN PHẨM
BẢO VỆ TRẺ EM TRÊN MÔI TRƯỜNG MẠNG**

BASIC TECHNICAL REQUIREMENTS FOR PRODUCTS PROTECTING CHILDREN ONLINE

HÀ NỘI – 2024

Mục lục

Lời nói đầu.....	3
Lời giới thiệu.....	4
1. Phạm vi, đối tượng áp dụng.....	5
<i>1.1. Phạm vi áp dụng.....</i>	<i>5</i>
<i>1.2. Đối tượng áp dụng.....</i>	<i>5</i>
2. Thuật ngữ và định nghĩa.....	5
<i>2.1. Bảo vệ trẻ em trên môi trường mạng.....</i>	<i>5</i>
<i>2.2. Sản phẩm bảo vệ trẻ em trên môi trường mạng.....</i>	<i>5</i>
<i>2.3. Nội dung không phù hợp, độc hại cho trẻ em.....</i>	<i>6</i>
<i>2.4. Danh sách đen.....</i>	<i>6</i>
<i>2.5. Dữ liệu cá nhân.....</i>	<i>6</i>
3.1. Yêu cầu về tài liệu và chính sách.....	6
<i>3.1.1. Về tài liệu hướng dẫn người dùng.....</i>	<i>6</i>
<i>3.1.2. Về chính sách.....</i>	<i>6</i>
<i>3.2.1. Lọc nội dung.....</i>	<i>7</i>
<i>3.2.2. Kiểm soát sử dụng.....</i>	<i>7</i>
<i>3.2.3. Giám sát.....</i>	<i>8</i>
<i>3.2.4. Nền tảng triển khai sản phẩm.....</i>	<i>9</i>
3.3. Yêu cầu về tính tuân thủ và đặc thù Việt Nam.....	9
<i>3.3.1. Cập nhật dữ liệu Việt Nam.....</i>	<i>9</i>
<i>3.3.2. Phản ánh thông tin, dịch vụ gây hại cho trẻ em.....</i>	<i>9</i>
3.4. Yêu cầu về yếu tố an toàn thông tin của của doanh nghiệp và hệ thống.....	9
<i>3.4.1. Bảo vệ dữ liệu cá nhân.....</i>	<i>9</i>
<i>3.4.2. Đánh giá an toàn thông tin.....</i>	<i>9</i>
<i>3.4.3. Đáp ứng yêu cầu an toàn theo cấp độ.....</i>	<i>9</i>
3.5. Yêu cầu về hiệu năng xử lý.....	10
<i>3.5.1. Đối với Thiết bị phần cứng mạng.....</i>	<i>10</i>
<i>3.5.2. Đối với Sản phẩm phần mềm.....</i>	<i>10</i>
Phụ lục A: Tiêu chí đánh giá về tài liệu.....	11
Phụ lục B: Tiêu chí đánh giá về tính năng.....	13
Phụ lục C: Tiêu chí đánh giá về tính tuân thủ.....	17
Phụ lục D: Tiêu chí đánh giá về an toàn thông tin.....	18
Phụ lục E: Tiêu chí đánh giá về hiệu năng.....	21

Lời nói đầu

TCCS 03:2024/VNISA được xây dựng trên cơ sở thực tiễn triển khai các sản phẩm bảo vệ trẻ em trên môi trường mạng tại Việt Nam, có tham khảo các sản phẩm, tài liệu trong nước và quốc tế.

TCCS 03:2024/VNISA được Hiệp hội An toàn thông tin Việt Nam (VNISA) giao cho Câu lạc bộ Bảo vệ trẻ em Việt Nam trên không gian mạng (VCSC) biên soạn; lấy ý kiến các cơ quan, tổ chức có liên quan; tổ chức thẩm định và công bố.

Quá trình xây dựng TCCS, VNISA được sự hỗ trợ của Tổ chức Tầm Nhìn Thế giới tại Việt Nam (World Vision Việt Nam) và Đại diện Tổ chức ChildFund Australia tại Việt Nam (ChildFund Việt Nam).

Lời giới thiệu

Tiêu chuẩn này quy định các yêu cầu kỹ thuật cơ bản đối với sản phẩm bảo vệ trẻ em trên môi trường mạng, bao gồm 5 nhóm: *Yêu cầu về tài liệu; Yêu cầu về tính năng; Yêu cầu về tính tuân thủ và đặc thù Việt Nam; Yêu cầu về yếu tố an toàn thông tin của sản phẩm; Yêu cầu về hiệu năng xử lý.*

Các yêu cầu nêu trong Tiêu chuẩn cơ sở này là yêu cầu cơ bản đối với việc xây dựng sản phẩm bảo vệ trẻ em trên môi trường mạng. Khuyến khích các tổ chức, doanh nghiệp bổ sung thêm các yêu cầu ở cấp độ cao hơn nhằm nâng cao chất lượng sản phẩm, dịch vụ.

Các yêu cầu nêu trong nội dung Tiêu chuẩn là căn cứ cho việc đánh giá chất lượng sản phẩm bảo vệ trẻ em trên môi trường mạng.

YÊU CẦU KỸ THUẬT CƠ BẢN ĐỐI VỚI SẢN PHẨM BẢO VỆ TRẺ EM TRÊN MÔI TRƯỜNG MẠNG

1. Phạm vi, đối tượng áp dụng

1.1. Phạm vi áp dụng

Tiêu chuẩn này quy định các yêu cầu kỹ thuật cơ bản đối với sản phẩm Bảo vệ trẻ em trên môi trường mạng (BVTE). Tài liệu bao gồm các nội dung: *Yêu cầu về tài liệu; Yêu cầu về tính năng; Yêu cầu về tính tuân thủ và hiệu quả; Yêu cầu về yếu tố an toàn thông tin của sản phẩm; Yêu cầu về hiệu năng xử lý.*

1.2. Đối tượng áp dụng

Các cơ quan, tổ chức, cá nhân có liên quan đến hoạt động nghiên cứu, phát triển; đánh giá, lựa chọn sản phẩm BVTE khi đưa vào sử dụng.

2. Thuật ngữ và định nghĩa

Trong tài liệu này các khái niệm và thuật ngữ được hiểu như sau

2.1. Bảo vệ trẻ em trên môi trường mạng

Bảo vệ trẻ em trên môi trường mạng (hay còn gọi là bảo vệ trẻ em trên không gian mạng, bảo vệ trẻ em trên môi trường trực tuyến) là việc thực hiện các biện pháp và hành động phù hợp nhằm bảo đảm trẻ được an toàn khi sử dụng Internet và các dịch vụ trực tuyến, bao gồm các hoạt động giáo dục nhận thức; phòng ngừa, phát hiện, xử lý, ngăn chặn các hành vi xâm hại trẻ em trên không gian mạng và các nguy cơ khác gây tổn hại cho trẻ em trên không gian mạng.

2.2. Sản phẩm bảo vệ trẻ em trên môi trường mạng

- a) Thiết bị phân cứng mạng: Là giải pháp bảo vệ trẻ em sử dụng thiết bị mạng độc lập với các thiết bị cần giám sát, bảo vệ (máy tính, điện thoại...). Thiết bị mạng độc lập này đóng vai trò là cửa ngõ (gateway) của các thiết bị cần giám sát, bảo vệ.
- b) Phần mềm và các tiện ích mở rộng (gọi tắt là phần mềm): Là giải pháp bảo vệ trẻ em theo hình thức cài đặt thêm các phần mềm, thành phần bổ sung (add-on) vào thiết bị cần giám sát, bảo vệ (máy tính, điện thoại...).

c) Sản phẩm bảo vệ trẻ em gồm có các Thiết bị phần cứng mạng, phần mềm và các tiện ích mở rộng và hệ thống quản lý tập trung (máy chủ, phần mềm quản lý) của nhà cung cấp dịch vụ.

2.3. Nội dung không phù hợp, độc hại cho trẻ em

Là những thông tin có thể trực tiếp hoặc có nguy cơ gây tổn hại tới thể chất, tinh cảm, tâm lý, danh dự, nhân phẩm và sự phát triển lành mạnh của trẻ em, bao gồm thông tin giả mạo, sai sự thật; cổ súy các hủ tục, mê tín, dị đoan, dâm ô, đồi trụy; miêu tả tỉ mỉ hành động chém giết, tai nạn, kinh dị, rùng rợn; hàng hoá, dịch vụ bị cấm, các trò chơi, thử thách nguy hiểm và các thông tin khác không phù hợp với thuần phong, mỹ tục của dân tộc, tái quy định của pháp luật.

2.4. Danh sách đen

Danh sách địa chỉ/dải địa chỉ IP hoặc đường dẫn trang web (URL) được coi là không tin cậy hoặc chứa nội dung không phù hợp, độc hại, bị ngăn chặn truy cập bởi giải pháp BVTE.

2.5. Dữ liệu cá nhân

Là các dữ liệu do người dùng cung cấp, thao tác trong quá trình sử dụng sản phẩm bảo vệ trẻ em gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể, bao gồm (nhưng không giới hạn) các thông tin như: Tên, tuổi, địa chỉ, email, số điện thoại, lịch sử truy cập; từ khóa tìm kiếm...

3. Các yêu cầu

3.1. Yêu cầu về tài liệu và chính sách

3.1.1. Về tài liệu hướng dẫn sử dụng dành cho người dùng

Có tài liệu hướng dẫn sử dụng dành cho người dùng.

3.1.2. Về chính sách

a) Chính sách thu thập và xử lý dữ liệu cá nhân

Có chính sách thu thập và xử lý dữ liệu cá nhân, tuân thủ theo nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân.

b) Chính sách tiếp nhận và báo cáo lỗ hổng, điểm yếu

Có chính sách tiếp nhận và cảnh báo lỗ hổng, điểm yếu.

- c) Chính sách tiếp nhận các phản ánh về hiệu năng, tính năng sản phẩm
 Có chính sách tiếp nhận các phản ánh về hiệu năng, tính năng sản phẩm.

3.2. Yêu cầu về tính năng

3.2.1. Lọc nội dung

a) Tìm kiếm an toàn

Khi triển khai giải pháp BVTE, tại thiết bị được giám sát sẽ tự động kích hoạt chế độ tìm kiếm an toàn trên các nền tảng phổ biến (tối thiểu là Google, Bing, YouTube) hoặc tính năng duyệt web an toàn được cài đặt theo cấu hình của người dùng.

b) Ngăn chặn các trang web có nội dung không phù hợp, máy chủ của hệ thống mã độc, lừa đảo

Khi truy cập các trang web có chứa các nội dung không phù hợp, độc hại với trẻ em hoặc truy cập tới các máy chủ của các hệ thống mã độc, lừa đảo thì thiết bị được giám sát sẽ bị ngắt kết nối; hoặc sẽ chuyển tới một trang web có nội dung phù hợp; hoặc chuyển hướng sang 1 thông báo vi phạm.

Có giải pháp tối thiểu cập nhật mẫu nhận diện (website, máy chủ) từ Trung tâm giám sát an toàn không gian mạng Quốc gia (NCSC) hoặc từ các đơn vị tương đương.

c) Ngăn chặn/ cảnh báo việc cài đặt các ứng dụng có nội dung không phù hợp

- Đối với nhóm sản phẩm phần mềm có khả năng ngăn chặn hoặc cảnh báo tới người dùng khi người dùng có hành động cài đặt các ứng dụng, tiện ích đã có gán nhãn theo độ tuổi không phù hợp với trẻ em.

- Đối với các ứng dụng, tiện ích không gán nhãn thì có cảnh báo tới người dùng việc cài đặt có thể chứa những nội dung không phù hợp, độc hại với trẻ.

3.2.2. Kiểm soát sử dụng

a) Kiểm soát các thiết bị được bảo vệ

Sản phẩm BVTE có khả năng kiểm soát các thiết bị được bảo vệ về: trạng thái hoạt động (bật/tắt kết nối mạng), giới hạn thời gian hoạt động/kết nối mạng.

b) Kiểm soát ứng dụng (Tùy chọn)

Sản phẩm BVTE có khả năng kiểm soát các ứng dụng trên thiết bị bảo vệ: tên ứng dụng, giới hạn thời gian hoạt động cho phép.

c) Tự bảo vệ sản phẩm khi có sự can thiệp của người dùng (áp dụng với sản phẩm phần mềm)

Sản phẩm BVTE có khả năng cảnh báo/ngăn chặn các thao tác tắt hoặc đăng xuất, hoặc gỡ bỏ trên thiết bị bảo vệ.

d) Quản lý danh sách đen

Sản phẩm BVTE có cơ chế và chức năng cho phép người dùng cập nhật báo cáo về các trang web đen, không phù hợp với trẻ em cho nhà cung cấp sản phẩm dịch vụ hoặc các cơ quan chức năng liên quan; hoặc có chức năng cho phép người dùng tự chặn các trang web đen.

e) Quản lý danh sách ứng dụng cho phép sử dụng (tùy chọn)

Đối với các phần mềm có thể có cơ chế quản lý ứng dụng được phép sử dụng, theo đó chỉ những ứng dụng có trong danh sách này mới được phép sử dụng.

f) Kiểm soát thời gian sử dụng trên thiết bị được bảo vệ

Sản phẩm BVTE cho phép thiết lập thời gian sử dụng trên thiết bị được bảo vệ đáp ứng ít nhất một trong các yêu cầu sau:

- Giới hạn tổng thời gian sử dụng.
- Giới hạn theo các mốc thời gian sử dụng.

3.2.3. Giám sát

a) Đối với Thiết bị phần cứng mạng

Thống kê tình hình sử dụng: Cho phép giám sát tình hình sử dụng của tất cả các thiết bị trong mạng: thời lượng sử dụng của từng ứng dụng, của từng người/thiết bị.

b) Đối với Sản phẩm phần mềm

- Thống kê tình hình sử dụng: Cho phép giám sát trạng thái hoạt động trên thiết bị, thời lượng pin còn lại trên máy, thời gian cập nhật lần cuối.

- Theo dõi định vị: Cho phép theo dõi vị trí thiết bị được giám sát, bảo vệ theo thời gian, cập nhật vị trí cuối cùng của thiết bị được giám sát, bảo vệ (áp dụng cho việc cài đặt lên các thiết bị có chức năng định vị).
- Cảnh báo SOS: Cho phép gửi cảnh báo nguy hiểm từ thiết bị được giám sát bảo vệ đến thiết bị giám sát theo tình huống định sẵn hoặc sử dụng nút SOS (áp dụng cho việc cài đặt lên các thiết bị di động).

3.2.4. *Nền tảng triển khai sản phẩm*

Sản phẩm phần mềm: Cho phép các đặt trên các hệ điều hành phổ biến là: Windows, Android, iOS và các trình duyệt (nếu có).

3.3. *Yêu cầu về tính tuân thủ và đặc thù Việt Nam*

3.3.1. *Cập nhật dữ liệu Việt Nam*

Có cơ chế và thực hiện cập nhật dữ liệu bảo vệ (tên miền độc hại, lừa đảo ...) có đặc thù Việt Nam vào sản phẩm.

3.3.2. *Phản ánh thông tin, dịch vụ gây hại cho trẻ em, thông tin, dịch vụ giả mạo, xuyên tạc, xâm hại trẻ em trên môi trường mạng tới cơ quan quản lý chức năng.*

Thiết lập tính năng và tích hợp với hệ thống tiếp nhận phản ánh của Mạng lưới ứng cứu bảo vệ trẻ em trên môi trường mạng (<https://vn-cop.vn/bao-cao-xam-pham/>) để cho phép người sử dụng có thể thông báo các thông tin, dịch vụ gây hại cho trẻ em, thông tin, dịch vụ giả mạo, xuyên tạc, xâm hại trẻ em.

3.4. *Yêu cầu về yếu tố an toàn thông tin của của doanh nghiệp và hệ thống*

3.4.1. *Bảo vệ dữ liệu cá nhân*

Doanh nghiệp cung cấp sản phẩm BVTE thực hiện tuân thủ bảo vệ dữ liệu cá nhân theo Nghị định 13/2023/NĐ-CP.

3.4.2. *Đánh giá an toàn thông tin*

Hệ thống cung cấp sản phẩm BVTE (Thiết bị phần cứng mạng, phần mềm cài đặt bảo vệ và hệ thống quản lý tập trung) có thực hiện kiểm tra, đánh giá an toàn thông tin trước khi đi vào sử dụng.

3.4.3 *Đáp ứng yêu cầu an toàn theo cấp độ*

Hệ thống cung cấp sản phẩm BVTE thực hiện đảm bảo đáp ứng cấp độ 3 trở lên.

3.5. Yêu cầu về hiệu năng xử lý

3.5.1. Đối với Thiết bị phần cứng mạng

Độ trễ thời gian truy cập Internet không quá 10% so với khi không sử dụng sản phẩm BVTE.

3.5.2. Đối với Sản phẩm phần mềm

Mức sử dụng tài nguyên RAM, CPU không vượt quá các định mức thông thường của một phần mềm, cụ thể: mỗi tiến trình của phần mềm BVTE sử dụng không quá 500MB RAM và 15% CPU của thiết bị trong trạng thái hoạt động ở chế độ ẩn (trạng thái chưa có các thao tác chức năng trên phần mềm BVTE từ phía người dùng).

Phụ lục A: Tiêu chí đánh giá về tài liệu
(Quy định)

TT	Yêu cầu	Mô tả	Tiêu chí đánh giá, đo lường	Áp dụng cho
1	Về tài liệu hướng dẫn người dùng	Có tài liệu hướng dẫn sử dụng dành cho người dùng	<p>a) Tài liệu hướng dẫn được viết một cách rõ ràng và dễ hiểu, thực hiện theo tài liệu hướng dẫn sử dụng có thể sử dụng được các tính năng của sản phẩm. Có cấu trúc rõ ràng, bao gồm các phần như giới thiệu sản phẩm, hướng dẫn cài đặt, cách sử dụng các tính năng chính, và các câu hỏi thường gặp.</p> <p>b) Nếu sản phẩm được sử dụng ở nhiều quốc gia hoặc khu vực, tài liệu hướng dẫn cần có thêm ít nhất một ngôn ngữ là tiếng Anh.</p> <p>c) Tài liệu hướng dẫn được công bố công khai trên website chính thức của nhà cung cấp sản phẩm, dịch vụ hoặc bằng hình thức phù hợp (sách, tờ rơi Hướng dẫn sử dụng).</p>	Cả Thiết bị phần cứng mạng và phần mềm
2	Chính sách thu thập và xử lý dữ liệu cá nhân.	Có chính sách thu thập và xử lý dữ liệu cá nhân tuân thủ Nghị định 13/2023/NĐ-CP".	<p>a) Chính sách nên cung cấp thông tin chi tiết về mục đích của việc thu thập dữ liệu cá nhân, loại dữ liệu được thu thập, và cách thức sử dụng và bảo vệ dữ liệu.</p> <p>b) Chính sách cần mô tả rõ ràng về quyền của người dùng đối với việc thu thập và sử dụng dữ liệu cá nhân của họ, và đảm bảo rằng sự đồng ý của họ được thu thập một cách tự nguyện và rõ ràng.</p> <p>c) Chính sách nên đảm bảo rằng có các biện pháp bảo mật thích hợp được thực hiện để bảo vệ dữ liệu cá nhân khỏi mất mát, sử dụng trái phép, hoặc tiết lộ không đúng cách. (Sử dụng kết hợp với các yếu tố bảo mật trong mục 4)</p> <p>d) Chính sách cần xác định thời gian giữ lại dữ liệu cá nhân và quy trình xóa</p>	Cả Thiết bị phần cứng mạng và phần mềm

			<p>dữ liệu sau khi nó không còn cần thiết cho mục đích ban đầu.</p> <p>e) Chính sách nên mô tả các quyền của người dùng, bao gồm quyền truy cập, chỉnh sửa, xoá, hoặc chuyển dữ liệu cá nhân của họ.</p>	
3	Chính sách tiếp nhận và báo cáo lỗ hổng, điểm yếu	<p>Có chính sách tiếp nhận và cảnh báo lỗ hổng, điểm yếu phù hợp với điều kiện hoạt động của nhà cung cấp sản phẩm, dịch vụ. Chính sách được công khai trên trang web chính thức của nhà cung cấp sản phẩm, dịch vụ hoặc bằng hình thức phù hợp.</p>	<p>a) Chính sách cần mô tả rõ ràng quy trình tiếp nhận lỗ hổng bao gồm cách thức người dùng hoặc bên thứ ba có thể báo cáo lỗ hổng và kênh giao tiếp được sử dụng.</p> <p>b) Chính sách nên đề ra một thời gian cụ thể mà tổ chức sẽ phản hồi sau khi nhận được báo cáo về lỗ hổng, đảm bảo rằng phản ứng được thực hiện kịp thời.</p> <p>c) Chính sách cần một cách rõ ràng định nghĩa các tiêu chí để phân loại và ưu tiên hóa các lỗ hổng dựa trên mức độ nghiêm trọng và tiềm năng ảnh hưởng.</p> <p>d) Chính sách nên mô tả quy trình phản hồi và giải quyết lỗ hổng, bao gồm việc xác nhận, đánh giá, và sửa chữa lỗ hổng một cách kịp thời.</p>	Cả Thiết bị phần cứng mạng và phần mềm
4	Chính sách tiếp nhận các phản ánh về hiệu năng, tính năng sản phẩm.	<p>Có cơ chế tiếp nhận phản ánh phù hợp với điều kiện hoạt động của nhà cung cấp</p> <p>Chính sách được công khai trên trang web chính thức của nhà cung cấp hoặc bằng hình thức phù hợp.</p>	<p>a) Chính sách cần xác định rõ các kênh mà người dùng hoặc bên liên quan có thể sử dụng để gửi phản ánh về hiệu năng và tính năng của sản phẩm.</p> <p>b) Chính sách nên đề ra một mức tiêu chuẩn về thời gian phản hồi sau khi nhận được phản ánh, đảm bảo rằng phản ứng được thực hiện kịp thời.</p> <p>c) Chính sách nên mô tả quy trình phản hồi và giải quyết phản ánh, bao gồm việc xác nhận, đánh giá, và xử lý các phản ánh một cách kịp thời và hiệu quả.</p>	Cả Thiết bị phần cứng mạng và phần mềm

Phụ lục B: Tiêu chí đánh giá về tính năng
(Quy định)

TT	Tính năng	Mô tả	Tiêu chí đánh giá, đo lường	Áp dụng cho
1	Tìm kiếm an toàn	Khi triển khai giải pháp BVTE, trên thiết bị được giám sát sẽ tự động kích hoạt chế độ tìm kiếm an toàn trên các nền tảng tìm kiếm phổ biến (tối thiểu là Google, Bing, YouTube) hoặc tính năng duyệt web an toàn được cài đặt theo cấu hình của người dùng.	Khi triển khai giải pháp BVTE, trên thiết bị được giám sát sẽ tự động kích hoạt chế độ tìm kiếm an toàn trên các nền tảng tìm kiếm phổ biến (search engine) mà không cần sự can thiệp của người dùng (tối thiểu là Google, Bing, YouTube) hoặc tính năng duyệt web an toàn được cài đặt theo cấu hình của người dùng.	Cả Thiết bị phần cứng mạng và phần mềm
2	Ngăn chặn các trang web có nội dung không phù hợp, máy chủ của hệ thống mã độc, lừa đảo.	<p>a) Khi truy cập các trang web có chứa các nội dung không phù hợp, độc hại với trẻ em hoặc truy cập tới các máy chủ của các hệ thống mã độc, lừa đảo thì thiết bị được giám sát sẽ:</p> <ul style="list-style-type: none"> + Hoặc sẽ bị ngắt kết nối, hoặc không truy cập được; + Hoặc sẽ chuyển tới một trang Web có nội dung phù hợp; + Hoặc chuyển hướng sang 1 thông báo vi phạm. <p>b) Giải pháp phần mềm BVTE phải cập nhật tối thiểu mẫu nhận diện (website, máy chủ) từ Trung tâm giám sát an toàn không gian mạng Quốc gia (NCSC) hoặc tương đương.</p>	<p>Khi truy cập các trang web có chứa các nội dung không phù hợp, độc hại với trẻ em hoặc truy cập tới các máy chủ của các hệ thống mã độc, lừa đảo sẽ bị ngắt kết nối hoặc chuyển hướng sang 1 thông báo vi phạm.</p> <p>Giải pháp tối thiểu cập nhật mẫu nhận diện (website, máy chủ) từ Trung tâm giám sát an toàn không gian mạng Quốc gia (NCSC): thử nghiệm 5 mẫu nhận diện từ NCSC để đánh giá hiệu quả.</p>	Cả Thiết bị phần cứng mạng và phần mềm

3	Ngăn chặn/cảnh báo việc cài đặt các ứng dụng có nội dung không phù hợp	<p>Đối với nhóm sản phẩm có khả năng ngăn chặn hoặc cảnh báo tới người dùng khi người dùng có hành động cài đặt các ứng dụng, tiện ích đã có gán nhãn theo độ tuổi không phù hợp với trẻ em.</p> <p>Đối với các ứng dụng, tiện ích không gán nhãn thì có cảnh báo tới người dùng việc cài đặt có thể chứa những nội dung không phù hợp, độc hại với trẻ.</p>	<p>a) Sản phẩm BVTE ngăn chặn hoặc cảnh báo 100% việc cài đặt các ứng dụng, tiện ích có gán nhãn độ tuổi không phù hợp với trẻ em (Áp dụng đối với sản phẩm cài đặt trên thiết bị di động Android, iOS).</p> <p>b) Sản phẩm BVTE có chức năng cảnh báo một số ứng dụng không gán nhãn độ tuổi có thể chứa nội dung không phù hợp, độc hại với trẻ.</p> <p>Đối với sản phẩm trên nền tảng iOS: không bắt buộc có tính năng này.</p>	Phần mềm
4	Kiểm soát các thiết bị được bảo vệ	Sản phẩm BVTE có khả năng kiểm soát các thiết bị được bảo vệ: trạng thái bật/tắt kết nối mạng, giới hạn thời gian hoạt động cho phép.	<p>a) Sản phẩm BVTE có giao diện thiết lập thời gian hoạt động cho phép.</p> <p>b) Sản phẩm BVTE có chức năng ngăn cản hoạt động bình thường của trẻ em với thiết bị khi hết thời gian cho phép.</p> <p>c) Sản phẩm BVTE có chức năng cho phép phụ huynh xác nhận để mở lại kết nối mạng cho thiết bị.</p>	Cả Thiết bị phần cứng mạng và phần mềm
5	Kiểm soát ứng dụng (Tùy chọn)	Sản phẩm BVTE có khả năng kiểm soát các ứng dụng trên thiết bị bảo vệ: tên ứng dụng, giới hạn thời gian hoạt động cho phép.	Đánh giá khả năng của sản phẩm BVTE trong việc nhận diện và kiểm soát các ứng dụng được cài đặt trên thiết bị: cho phép/ không cho phép sử dụng, giới hạn thời gian sử dụng.	Cả Thiết bị phần cứng mạng và phần mềm

6	Tự bảo vệ sản phẩm khi có sự can thiệp của người dùng	Sản phẩm BVTE có khả năng cảnh báo/hoặc ngăn chặn các thao tác tắt hoặc đăng xuất hoặc gỡ bỏ trên thiết bị được giám sát, bảo vệ.	<p>Đối với sản phẩm trên Windows:</p> <p>a) Phần mềm BVTE có khả năng ngăn chặn/cảnh báo việc dừng tiến trình hoạt động của phần mềm BVTE từ phía người dùng và các ứng dụng khác.</p> <p>b) Phần mềm BVTE có khả năng ngăn chặn/cảnh báo việc can thiệp thay đổi trái phép nội dung file, cấu hình phần mềm BVTE từ phía người dùng và các ứng dụng khác.</p> <p>c) Phần mềm BVTE có chức năng chống việc tự ý gỡ bỏ phần mềm BVTE, yêu cầu xác nhận của cha mẹ trước khi gỡ bỏ.</p> <p>Đối với sản phẩm trên iOS: không bắt buộc có tính năng này.</p>	Phần mềm
7	Quản lý danh sách đen các kết nối	Sản phẩm BVTE có cơ chế và chức năng cho phép người dùng cập nhật báo cáo về các trang web đen, không phù hợp với trẻ em cho nhà cung cấp sản phẩm dịch vụ hoặc các cơ quan chức năng liên quan; hoặc có chức năng cho phép người dùng tự chặn các trang web đen.	Sản phẩm BVTE có chức năng cập nhật danh sách đen cho người dùng; hoặc có chức năng cho phép người dùng tự chặn các trang web đen.	Cả Thiết bị phần cứng mạng và phần mềm
8	Kiểm soát thời gian sử dụng trên thiết bị được bảo vệ	Sản phẩm BVTE cho phép thiết lập thời gian sử dụng trên thiết bị được bảo vệ đáp ứng ít nhất một trong các yêu cầu sau: - Giới hạn tổng thời gian sử dụng;	Sản phẩm có khả năng giới hạn tổng thời gian sử dụng thiết bị hoặc thiết lập các mốc thời gian sử dụng cụ thể.	Cả Thiết bị phần cứng mạng và phần mềm

		- Giới hạn theo các mốc thời gian sử dụng.		
9	Tính năng giám sát của Thiết bị phần cứng mạng	Thống kê tình hình sử dụng: Cho phép giám sát tình hình sử dụng tất cả các thiết bị trong mạng: thời lượng sử dụng của từng ứng dụng, của từng người/thiết bị.	Đảm bảo rằng sản phẩm có khả năng thu thập đầy đủ và chính xác thông tin về thời lượng sử dụng của từng ứng dụng và từng người/thiết bị trong mạng theo thời gian thực.	Thiết bị phần cứng mạng
10	Tính năng giám sát của phần mềm	Thống kê tình hình sử dụng: Cho phép giám sát trạng thái hoạt động trên thiết bị, thời lượng pin còn lại trên máy, thời gian cập nhật lần cuối. - Theo dõi định vị: Cho phép theo dõi vị trí thiết bị được giám sát, bảo vệ theo thời gian, cập nhật vị trí cuối cùng của thiết bị được giám sát, bảo vệ (áp dụng cho việc cài đặt lên các thiết bị có chức năng định vị). - Cảnh báo SOS: Cho phép gửi cảnh báo nguy hiểm từ thiết bị được giám sát bảo vệ đến thiết bị giám sát theo tình huống định sẵn hoặc sử dụng nút SOS (áp dụng cho việc cài đặt lên các thiết bị di động).	a) Phần mềm BVTE có chức năng hiển thị thời lượng pin, thời gian cập nhật cuối. b) Với các thiết bị có chức năng định vị, phần mềm BVTE có chức năng cho phép người dùng cấu hình địa chỉ nhận thông tin định vị và gửi thông tin vị trí thiết bị về địa chỉ đã cấu hình. c) Với các thiết bị di động: Phần mềm BVTE có chức năng gửi cảnh báo nguy hiểm tới địa chỉ được cấu hình. Chức năng được kích hoạt trong 2 tình huống: Trẻ em chủ động ấn nút SOS trên giao diện hoặc thiết bị rơi vào tình huống được nhà phát triển cấu hình.	Phần mềm
11	Nền tảng triển khai sản phẩm	Sản phẩm phần mềm: Cho phép các đặt trên các hệ điều hành phổ biến là: Windows, Android, iOS và các trình duyệt (nếu có).	Phần mềm BVTE có các phiên bản cho các hệ điều hành phổ biến: Windows, Android, iOS và các trình duyệt (nếu có)	Phần mềm

Phụ lục C: Tiêu chí đánh giá về tính tuân thủ
(Quy định)

TT	Yêu cầu	Mô tả	Tiêu chí đánh giá, đo lường	Áp dụng cho
1	Cập nhật dữ liệu Việt Nam	Có cơ chế và thực hiện cập nhật dữ liệu dấu hiệu tấn công (tên miền độc hại, lừa đảo ...) có đặc thù Việt Nam vào sản phẩm.	Dữ liệu bảo vệ được cập nhật từ các nguồn thông tin đáng tin cậy về các mối đe dọa trực tuyến đặc thù của Việt Nam, bao gồm cả các cơ quan quản lý Nhà nước trong lĩnh vực an toàn, an ninh mạng tại Việt Nam và các nguồn tương đương (tối thiểu là thông tin từ Trung tâm giám sát An toàn không gian mạng Quốc gia - NCSC).	Cả Thiết bị phần cứng mạng và phần mềm
2	Phản ánh thông tin, dịch vụ gây hại cho trẻ em, thông tin, dịch vụ giả mạo, xuyên tạc, xâm hại trẻ em trên môi trường mạng tới cơ quan quản lý chức năng.	Thiết lập tính năng và tích hợp với hệ thống tiếp nhận phản ánh của Mạng lưới ứng cứu bảo vệ trẻ em trên môi trường mạng để cho phép người sử dụng có thể thông báo các thông tin, dịch vụ gây hại cho trẻ em, thông tin, dịch vụ giả mạo, xuyên tạc, xâm hại trẻ em.	Có chức năng gửi phản ánh lên Mạng lưới tại địa chỉ: https://vn-cop.vn/bao-cao-xam-pham/ .	Cả Thiết bị phần cứng mạng và phần mềm

Phụ lục D: Tiêu chí đánh giá về an toàn thông tin
(Quy định)

TT	Yêu cầu	Mô tả	Tiêu chí đánh giá, đo lường	Áp dụng cho
1	Bảo mật dữ liệu cá nhân	Doanh nghiệp thực hiện tuân thủ bảo vệ dữ liệu cá nhân theo Nghị định 13/2023/NĐ-CP. Công bố công khai chính sách trên trang web chính thức của nhà cung cấp sản phẩm, dịch vụ hoặc bằng hình thức phù hợp.	Đã thực hiện Báo cáo đánh giá tác động và gửi hồ sơ báo cáo đánh giá tác động bảo vệ dữ liệu cá nhân theo nghị định 13/2023/NĐ-CP.	
2	Đánh giá an toàn thông tin	Sản phẩm BVTE được thực hiện kiểm tra, đánh giá an toàn thông tin trước khi đi vào sử dụng	Hệ thống kỹ thuật cung cấp dịch vụ (ứng dụng mobile, web, máy chủ, API, thiết bị mạng, ứng dụng đầu cuối...) được đánh giá chứng nhận ATTT của một đơn vị có giấy phép kiểm tra, đánh giá an toàn thông tin mạng tại Việt Nam.	
3	Đáp ứng yêu cầu an toàn theo cấp độ	Doanh nghiệp có hồ sơ an toàn thông tin theo cấp độ	Doanh nghiệp xây dựng và phê duyệt (hoặc được phê duyệt) hồ sơ an toàn thông tin theo cấp độ, đáp ứng tối thiểu cấp độ 3	

Phụ lục E: Tiêu chí đánh giá về hiệu năng
(Quy định)

TT	Yêu cầu	Mô tả	Tiêu chí đánh giá, đo lường	Áp dụng cho
1	Đối với Thiết bị phần cứng mạng	Đối với Thiết bị phần cứng mạng: độ trễ thời gian truy cập Internet không quá 10% so với khi không sử dụng sản phẩm BVTE.	Khi sử dụng sản phẩm BVTE, tốc độ mạng không bị suy giảm quá 10% so với khi chưa sử dụng, Phương án kiểm tra: sử dụng công cụ đo tốc độ mạng của VNNIC để đo và tiến hành so sánh.	Thiết bị phần cứng mạng
2	Đối với sản phẩm phần mềm	Đối với sản phẩm phần mềm: mức tiêu tốn tài nguyên của mỗi tiến trình của phần mềm BVTE sử dụng không quá 500MB RAM và 15% CPU của máy tính trong trạng thái hoạt động ở chế độ ẩn.	Mức sử dụng tài nguyên RAM, CPU không vượt quá các định mức thông thường của một phần mềm. Cụ thể: mỗi tiến trình của phần mềm BVTE sử dụng không quá 500MB RAM và 15% CPU của thiết bị trong trạng thái hoạt động ở chế độ ẩn (trạng thái chưa có các thao tác chức năng trên phần mềm BVTE từ phía người dùng).	Phần mềm