TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 12822:2020

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN – HỒ SƠ BẢO VỆ CHO HỆ QUẢN TRỊ CƠ SỞ DỮ LIỆU

Information technology - Security techniques – Protection profile for database management systems

HÀ NỘI - 2020

Mục lục

1 Phạm vi áp dụng 7

2 Tài liệu viện dẫn 7

3 Thuật ngữ và định nghĩa 8

4 Ký hiệu và thuật ngữ viết tắt 12

5 Giới thiệu Hồ sơ bảo vệ 14

5.1 Tổng quan TOE 14

5.1.1 Định nghĩa TOE 15

5.1.2 Chức năng an toàn được TOE cung cấp 16

5.1.3 Chức năng an toàn tùy chọn 16

5.1.4 Môi trường vận hành TOE 17

5.2 Cấu hình PP 19

5.3 Quy ước 19

6 Các tuyên bố tuân thủ 19

6.1 Các yêu cầu phù hợp CC 19

6.2 Yêu cầu phù hợp với các gói 19

6.3 Yêu cầu phù hợp với các PP khác 19

6.4 Báo cáo phù hợp 20

7 Mô tả các vấn đề an toàn 20

7.1 Thảo luận không chính thức 20

7.2 Tài sản và các tác nhân đe dọa 20

7.3 Các mối đe dọa 20

7.4 Chính sách an toàn của tổ chức 21

7.5 Các giả định 23

8 Các mục tiêu an toàn 24

8.1 Các mục tiêu an toàn cho TOE 24

8.2 Các mục tiêu an toàn trong môi trường hoạt động 25

9 Yêu cầu chức năng an toàn mở rộng 26

10 Các yêu cầu an toàn 27
10.1 Các yêu cầu chức năng an toàn 27
10.1.1 Kiểm toán an toàn (FAU) 28
10.1.2 Bảo vệ dữ liệu người dùng (FDP) 31
10.1.3 Định danh và xác thực (FIA) 32
10.1.4 Quản lý an toàn (FMT) 34
10.1.5 Bảo vệ của TSF (FPT) 35
10.1.6 Truy cập TOE (FTA) 36
10.2 Các yêu cầu đảm bảo an toàn 36
11 Sở cứ 37
11.1 Sở cứ các mục tiêu an toàn TOE 37
11.1.1 Phạm vi mục tiêu an toàn TOE 38
11.1.2 Sở cứ các mục tiêu an toàn TOE 39
11.2 Sở cứ các mục tiêu an toàn cho môi trường hoạt động 49
11.3 Sở cứ các yêu cầu chức năng an toàn 63
11.3.1 Sở cứ các yêu cầu chức năng an toàn mở rộng 63
11.3.2 Sở cứ các yêu cầu chức năng an toàn TOE 64
11.3.3 Sở cứ đáp ứng các yêu cầu chức năng an toàn phụ thuộc 68
11.4 Sở cứ đáp ứng các yêu cầu bảo đảm an toàn 69
Thư mục tài liệu tham khảo 70

Lời nói đầu

TCVN 12822:2020 được xây dựng dựa trên cơ sở tham khảo "Protection Profile for Database Management Systems (DBMS PP) Base Package" của Hiệp hội đảm bảo thông tin quốc gia Mỹ (NIAP), phiên bản 2.12, ngày 23/3/2017.

TCVN 12822:2020 do Cục An toàn thông tin biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Công nghệ thông tin - Các kỹ thuật an toàn - Hồ sơ bảo vệ cho hệ quản trị cơ sở dữ liệu

Information Technology - Security techniques - Protection profile for Database Management Systems

1 Phạm vi áp dụng

Tiêu chuẩn này quy định hồ sơ bảo vệ cho các hệ quản trị cơ sở dữ liệu (gói cơ sở), thể hiện các yêu cầu chức năng an toàn (SFR) và các yêu cầu đảm bảo an toàn (SAR) đối với các hệ quản trị cơ sở dữ liệu (DBMS), phù hợp với bộ tiêu chuẩn quốc gia TCVN 8709-1:2011 (ISO/IEC 15408-1:2009), TCVN 8709-2:2011 (ISO/IEC 15408-2:2008) và TCVN 8709-3:2011 (ISO/IEC 15408-3:2008).

Các hệ quản trị cơ sở dữ liệu thuộc phạm vi áp dụng của tiêu chuẩn này là hệ quản trị cơ sở dữ liệu thương mại (COTS), được gọi chung là Đích đánh giá (TOE) và được quy định cụ thể tại điều 5.1.

Đích đánh giá (TOE) cung cấp kiểm soát truy cập phù hợp dựa trên định danh người dùng và nhóm thành viên (không bắt buộc), ví dụ: kiểm soát truy cập tùy quyền (DAC), và tạo bản ghi các sự kiện liên quan đến an toàn thông tin. Các quản trị viên có thẩm quyền của TOE được tin tưởng để không lạm dụng các đặc quyền được gán cho họ.

Đích an toàn (ST) phù hợp với tiêu chuẩn này phải đáp ứng tối thiểu tiêu chuẩn này theo hình thức tuân thủ có thể diễn giải như định nghĩa trong điều D.3 của tiêu chuẩn TCVN 8709-1:2011.

Hồ sơ bảo vệ này trong mục "mô tả vấn đề an toàn" (SPD) không bao gồm mục tiêu an toàn liên quan đến lịch sử truy cập.

Mặc dù nhiều tổ chức không chỉ định mục tiêu này là một phần của định nghĩa vấn đề an toàn của họ, mục tiêu an toàn bổ sung này có thể cần được đưa vào định nghĩa vấn đề an toàn của một số tổ chức để hỗ trợ giảm thiểu các mối đe dọa của T.ACCESS_TSFDATA và T.TSF_COMPROMISE. Điều này đạt được bằng cách cho phép người dùng được đào tạo xem lại lịch sử truy cập của họ để giúp xác định các nỗ lực truy cập trái phép.

Mục tiêu an toàn này có thể được tùy chọn đưa vào trong SPD bằng cách chỉ định cấu hình PP: Hồ sơ bảo vệ cho hệ thống quản lý cơ sở dữ liệu (Gói cơ sở) với Gói mở rộng DBMS PP- Lịch sử truy cập (DBMSPP-AH).

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau đây là cần thiết để áp dụng tiêu chuẩn này. Đối với tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất (bao gồm cả phiên bản sửa đổi, bổ sung).

TCVN 8709-1:2011 (ISO/IEC 15408-1:2009), "Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 1: Giới thiệu và mô hình tổng quát".

TCVN 8709-2:2011 (ISO/IEC 15408-2:2008), "Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 2: Các thành phần chức năng an toàn".

TCVN 8709-3:2011 (ISO/IEC 15408-3:2008), "Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 3: Các thành phần đảm bảo an toàn".

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa sau:

3.1

Truy cập (access)

Khả năng truy cập và sử dụng dữ liệu có trong hệ quản trị cơ sở dữ liệu.

3.2

Kiểm soát truy cập (access control)

Dịch vụ an toàn mà kiểm soát việc sử dụng các nguồn lực (phần cứng và phần mềm), việc tiết lộ và việc thay đổi dữ liệu (lưu trữ hoặc quảng bá).

3.3

Trách nhiệm giải trình (accountability)

Thuộc tính mà cho phép các hoạt động trong một hệ thống công nghệ thông tin có thể dò ra thực thể chịu trách nhiệm cho hoạt động nào đó.

3.4

Quản trị viên (administrator)

Một người dùng đã được trao quyền cụ thể để quản lý một số phần hoặc toàn bộ TOE và hành động của mình có thể ảnh hưởng đến TSP. Quản trị viên có thể có các đặc quyền đặc biệt cung cấp khả năng để ghi đè lên một phần của TSP.

3.5

Đảm bảo (assurance)

Một thước đo của sự tự tin rằng các tính năng an toàn của một hệ thống công nghệ thông tin là đủ để thực thi chính sách an toàn của nó.

3.6

Tấn công (attack)

Hành vi cố ý vi phạm chính sách an toàn của một hệ thống công nghệ thông tin.

3.7

Xác thực (authentication)

Phương pháp an toàn để xác thực người sử dụng hợp lệ.

3.8

Dữ liệu xác thực (authentication data)

Thông tin để xác minh người dùng hợp lệ.

3.9

Phân quyền (authorization)

Các quyền khác nhau được cấp cho từng quản trị viên của cơ sở dữ liệu (đọc/ghi/sửa/xóa...).

3.10

Quản trị viên có thẩm quyền (authorized administrator)

Người có thẩm quyền quản lý và chịu trách nhiệm duy trì khả năng hoạt động của TOE.

3.11

Người dùng được ủy quyền (authorized user)

Người có thể thực hiện một hoạt động theo TSP.

3.12

Tính sẵn sàng (availability)

Khả năng truy cập kịp thời (dựa theo một số liệu xác định được), tin cậy vào các tài nguyên công nghệ thông tin.

3.13

Phá hoại (compromise)

Sự vi phạm các chính sách an toàn.

3.14

Tính bí mật (confidentiality)

Một chính sách an toàn liên quan đến việc tiết lộ dữ liệu.

3.15

Dữ liệu cấu hình (configuration data)

Dữ liệu được sử dụng để cấu hình TOE.

3.16

Hệ quản trị cơ sở dữ liệu - DBMS (Database Management System – DBMS)

Một hệ thống quản lý cơ sở dữ liệu (DBMS) là phần mềm hệ thống để tạo và quản lý cơ sở dữ liệu, cung cấp khả năng tạo, truy xuất, cập nhật và quản lý dữ liệu. DBMS đóng vai trò là giao diện giữa cơ sở dữ liệu và người dùng cuối hoặc các chương trình ứng dụng, đảm bảo dữ liệu được tổ chức nhất quán và vẫn có thể truy cập dễ dàng.

3.17

Kiểm soát truy cập tùy quyền (Discretionary Access Control – DAC)

Một phương pháp nhằm hạn chế truy cập của các đối tượng trên cơ sở nhận dạng các đối tượng hoặc nhóm mà đối tượng trực thuộc. Phương pháp kiểm soát này được coi là tùy quyền bởi vì khi một chủ thể với sự cho phép truy cập nhất định nào đấy thì có thể chuyển quyền truy cập đó (trực tiếp hoặc gián tiếp) sang bất cứ một chủ thể nào khác trong hệ thống.

3.18

Vùng bao (enclave)

Một tập hợp các thực thể dưới sự kiểm soát của một cơ quan duy nhất và có một chính sách an toàn đồng nhất. Chúng có thể được truy cập từ xa để đọc, xem nhưng không thể tải xuống hoặc xóa từ máy chủ vật lý.

3.19

Thực thể (entity)

Một chủ thể, đối tượng, người dùng hoặc một thiết bị công nghệ thông tin, trong đó tương tác với các đối tượng, dữ liệu hoặc tài nguyên TOE.

3.20

Mã thực thi trong TSF (executable code within the TSF)

Phần mềm tạo nên TSF dưới dạng có thể chạy bằng máy tính.

3.21

Thực thể CNTT bên ngoài (external IT entity)

Bất kỳ sản phẩm hoặc hệ thống công nghệ thông tin (CNTT) nào được tin cậy, bên ngoài TOE, có thể thực hiện một hoạt động nào đó phù hợp với TSP.

3.22

Định danh (identity)

Một đại diện (ví dụ: một chuỗi) xác định duy nhất một người dùng được ủy quyền, có thể là tên đầy đủ/viết tắt của người dùng đó hoặc biệt hiệu.

3.23

Tính toàn vẹn (integrity)

Một chính sách an toàn liên quan đến sự thay đổi của dữ liệu và cơ chế TSF.

3.24

Đối tượng được đặt tên (named object)

Một đối tượng thể hiện tất cả các đặc điểm sau:

- Đối tượng có thể được sử dụng để truyền tải thông tin giữa người dùng và/hoặc nhóm khác nhau trong TSF.
- Các chủ thể trong TOE có khả năng yêu cầu một biểu hiện cụ thể của đối tượng.
- Tên được dùng để chỉ một biểu hiện cụ thể của đối tượng. Nó phải tồn tại trong một ngữ cảnh và có khả năng cho phép người dùng và/hoặc nhóm khác nhau yêu cầu cùng một biểu hiện của đối tượng.

3.25

Đối tượng (object)

Một thực thể trong TSC có lưu hoặc nhận thông tin về hoạt động của đối tượng.

3.26

Môi trường hoạt động (operating environment)

Toàn bộ môi trường mà một TOE vận hành. Nó bao gồm các cơ sở vật chất và bất cứ sự kiểm soát vật lý, thủ tục, hành chính và nhân sự nào.

3.27

Đối tượng công khai (public object)

Một đối tượng mà TSF cho phép tất cả các thực thể có thể truy cập quyền đọc vô điều kiện. Chỉ có TSF hoặc quản trị viên có thẩm quyền mới có thể tạo, xóa, hoặc sửa đổi các đối tượng công khai.

3.28

Trạng thái an toàn (secure state)

Điều kiện trong đó tất cả các chính sách an toàn TOE được thi hành.

3.29

Các thuộc tính an toàn (security attributes)

Dữ liệu TSF liên quan đến các đối tượng, chủ thể và người dùng được sử dụng để thực thi TSP.

3.30

Mức độ an toàn (security level)

Thước đo độ an toàn thông tin có trong cơ sở dữ liệu

3.31

Thông tin nhạy cảm (sensitive information)

Thông tin được xác định bởi cơ quan có thẩm quyền là nhạy cảm. Việc tiết lộ, thay đổi, mất mát, hoặc hủy hoại nó một cách trái phép sẽ gây ra thiệt hại cho một người hoặc vật nào đó.

3.32

Chủ thể (subject)

Một thực thể trong TSC làm cho hoạt động được thực hiện.

3.33

Mối đe dọa (threat)

Khả năng, ý định và phương pháp tấn công, hoặc bất kỳ trường hợp, sự kiện nào có khả năng vi phạm chính sách an toàn của TOE.

3.34

Tài nguyên TOE (TOE resources)

Bất cứ thứ gì có thể sử dụng hoặc tiêu hao trong TOE.

3.35

Người dùng chưa được ủy quyền (unauthorized user)

Một người dùng chỉ được truy cập vào các đối tượng công khai được cung cấp bởi hệ thống nếu có.

3.36

Người dùng (user)

Bất cứ thực thể (con người hoặc thực thể CNTT bên ngoài) nằm ngoài TOE có tương tác đến TOE.

3.37

Lỗ hổng (vulnerability)

Một điểm yếu có thể bị khai thác để vi phạm chính sách an toàn TOE.

4 Ký hiệu và thuật ngữ viết tắt

AH	Access History	Lịch sử truy cập
CA	Certificate Authority	Tổ chức chứng thực

CC	Common Criteria	Tiêu chuẩn chung
CNTT		Công nghệ thông tin
CM	Configuration Management	Quản lý cấu hình
COTS	Commercial Off The Shelf	Đóng gói sẵn để thương mại hóa
DAC	Discretionary Access Control	Kiểm soát truy cập tùy quyền
DBMS	Database Management System	Hệ quản trị cơ sở dữ liệu
DBMS PP	Database Management System Protection Profile	Hồ sơ bảo vệ cho hệ quản trị cơ sở dữ liệu
EAL	Evaluation Assurance Level	Cấp độ đảm bảo đánh giá
EP	Extended Package	Gói mở rộng
I&A	Identification and Authentication	Định danh và xác thực
IT	Information Technology	Công nghệ thông tin
LAN	Local Area network	Mạng nội bộ
OS	Operating System	Hệ điều hành
OSP	Organizational Security Policy	Chính sách an toàn của tổ chức
PP	Protection Profile	Hồ sơ bảo vệ
SAR	Security Assurance Requirement	Yêu cầu đảm bảo an toàn
SFP	Security Functional Policies	Chính sách chức năng an toàn
SFR	Security Functional Requirement	Yêu cầu chức năng an toàn
SPD	Security Problem Definition	Định nghĩa vấn đề an toàn
ST	Security Target	Đích an toàn
TOE	Target of Evaluation	Đích đánh giá
TSC	TSF Scope of Control	Phạm vi kiểm soát TSF
TSE	TOE Security Environment	Môi trường an toàn TOE
TSF	TOE Security Functions	Chức năng an toàn TOE
TSFI	TSF Interfaces	Giao diện TSF
TSP	TOE Security Policy	Chính sách an toàn TOE

5 Giới thiệu Hồ sơ bảo vệ

5.1 Tổng quan TOE

Loại sản phẩm đích đánh giá (TOE) được mô tả trong tiêu chuẩn này là hệ quản trị cơ sở dữ liệu (DBMS).

Một hệ quản trị cơ sở dữ liệu là một hệ thống máy tính mà lưu trữ thông tin và cho phép người dùng được ủy quyền thay đổi các thông tin đó. Một hệ quản trị cơ sở dữ liệu có thể là một hệ thống một người dùng, là hệ thống mà chỉ cho phép một người dùng truy cập vào tại một thời điểm nhất định, hoặc hệ thống đa người dùng, là hệ thống cho phép nhiều người dùng truy cập đồng thời.

Hệ quản trị cơ sở dữ liệu có khả năng hạn chế truy cập đối với người dùng được ủy quyền, thực thi kiểm soát truy cập tùy quyền DAC trên các đối tượng dựa vào người dùng và nhóm người dùng dưới sự kiểm soát của hệ quản trị cơ sở dữ liệu, và giúp xác định trách nhiệm của người dùng thông qua việc kiểm toán các hoạt động của người dùng.

Một hệ quản trị cơ sở dữ liệu bao gồm ứng dụng máy chủ hệ quản trị cơ sở dữ liệu thực hiện một hay nhiều tính năng dưới đây:

a. *Kiểm soát truy cập người dùng đến dữ liệu người dùng và dữ liệu hệ quản trị cơ sở dữ liệu;*

b. Tương tác và có thể bổ sung các phần của hệ điều hành nằm dưới để truy xuất và trình bày dữ liệu thuộc quản lý của hệ quản trị cơ sở dữ liệu;

c. Lập chỉ mục các giá trị dữ liệu với vị trí thực của chúng để truy xuất nhanh dựa trên một hoặc nhiều giá trị;

d. Thực thi các chương trình viết sẵn (ví dụ: các tiện ích...) để hoàn thành các tác vụ thông thường như sao lưu cơ sở dữ liệu, phục hồi, tải và sao chép;

e. Hỗ trợ cơ chế cho phép truy cập cơ sở dữ liệu đồng thời (ví dụ: các khóa...);

f. Giúp phục hồi dữ liệu người dùng và dữ liệu của hệ quản trị cơ sở dữ liệu (ví dụ: nhật ký giao dịch...);

g. Theo dõi hoạt động mà người dùng đã thực hiện;

Hầu hết các ứng dụng máy chủ hệ quản trị cơ sở dữ liệu thương mại đều cung cấp các chức năng dưới đây:

- *Một mô hình dữ liệu mà cùng với nó, các cấu trúc dữ liệu của hệ quản trị cơ sở dữ liệu và tổ chức có thể được khái niệm hóa (ví dụ: các mô hình dữ liệu phân tầng, hướng đối tượng hay mô hình dữ liệu quan hệ...) và các đối tượng của hệ quản trị cơ sở dữ liệu được định nghĩa.*
- Ngôn ngữ bậc cao hoặc các giao diện cho phép những người dùng được ủy quyền định nghĩa kiến trúc cơ sở dữ liệu; truy cập và thay đổi dữ liệu người dùng hoặc dữ liệu hệ quản trị cơ sở

dữ liệu; trình bày dữ liệu người dùng và dữ liệu hệ quản trị cơ sở dữ liệu; và thực thi các hành động với những dữ liệu đó.

Một hệ quản trị cơ sở dữ liệu chủ yếu chia ra 2 kiểu người dùng:

- Những người dùng tương tác với hệ quản trị cơ sở dữ liệu để xem và thay đổi các đối tượng dữ liệu mà họ có quyền để truy cập.
- Các quản trị viên được ủy quyền là những người thực thi và quản lý các chính sách liên quan đến thông tin của một tổ chức (ví dụ: khả năng truy cập, tính toàn vẹn, tính nhất quán, tính sẵn sàng) cho cơ sở dữ liệu mà họ cài đặt, cấu hình, quản lý và/hoặc sở hữu.

Một hệ quản trị cơ sở dữ liệu lưu trữ và kiểm soát truy cập đối với 2 loại dữ liệu sau:

- Loại thứ nhất là dữ liệu người dùng được hệ quản trị cơ sở dữ liệu duy trì và bảo vệ. Dữ liệu người dùng có thể bao gồm những đặc điểm sau:

a. Dữ liệu người dùng được lưu trữ trong các đối tượng cơ sở dữ liệu hoặc là các đối tượng cơ sở dữ liệu.

b. Những định nghĩa về các cơ sở dữ liệu người dùng và đối tượng cơ sở dữ liệu thường được biết đến như là dữ liệu đặc tả – metadata.

c. Những truy vấn từ phía người dùng, chức năng, hay thủ tục mà hệ quản trị cơ sở dữ liệu duy trì cho người dùng.

- Loại thứ hai là dữ liệu hệ quản trị cơ sở dữ liệu (ví dụ: thông số cấu hình, thuộc tính an ninh của người dùng, nhật ký giao dịch, chỉ dẫn kiểm toán, và các bản ghi) mà hệ quản trị cơ sở dữ liệu duy trì và có thể sử dụng để vận hành hệ quản trị cơ sở dữ liệu.

Những đặc điểm của hệ quản trị cơ sở dữ liệu xác định những yêu cầu chi tiết cho các chức năng hoạt động của hệ quản trị cơ sở dữ liệu được đưa ra với danh sách trên.

5.1.1 Định nghĩa TOE

Đích đánh giá bao gồm ít nhất một trường hợp về các chức năng an toàn (ví dụ: kỹ thuật cơ sở dữ liệu...) của ứng dụng máy chủ hệ quản trị cơ sở dữ liệu cùng với các tài liệu hướng dẫn liên quan của nó và các giao diện để các thực thể IT bên ngoài có thể tương tác với hệ quản trị cơ sở dữ liệu.

Tài liệu này không bắt buộc áp dụng với một kiến trúc cụ thể. Tác giả ST sẽ cần xác định và mô tả kiến trúc của TOE cần đánh giá.

Các thực thể IT bên ngoài mà tương tác với hệ quản trị cơ sở dữ liệu, không nằm trong đích đánh giá, bao gồm:

- Ứng dụng khách cho phép người dùng tương tác với máy chủ hệ quản trị cơ sở dữ liệu.
- Hệ điều hành mà đích đánh giá được cài đặt.

- Các thiết bị mạng, in, lưu trữ dữ liệu, các thiết bị khác và các dịch vụ mà hệ điều hành có thể tương tác thay cho hệ quản trị cơ sở dữ liệu hoặc người dùng hệ quản trị cơ sở dữ liệu. Các sản phẩm IT khác như máy chủ ứng dụng, máy chủ web, máy chủ xác thực, máy chủ thư mục, máy chủ kiểm toán, và hệ thống xử lý giao dịch mà hệ quản trị cơ sở dữ liệu có thể tương tác để thực thi các chức năng quản trị cơ sở dữ liệu hoặc chức năng an toàn.

Nếu hệ điều hành máy chủ nằm ngoài phạm vi của TOE, hệ quản trị cơ sở dữ liệu phải xác định hệ điều hành mà nó được cài đặt lên để cung cấp mức độ tích hợp các tính năng an toàn mong muốn cũng như các cấu hình mà hệ điều hành cần có để hỗ trợ các tính năng an toàn của hệ quản trị cơ sở dữ liệu. Tuy nhiên, các mục tiêu về tính bí mật, tính toàn vẹn và tính sẵn sàng cho TOE phải được đáp ứng bởi toàn bộ hệ thống: hệ quản trị cơ sở dữ liệu và các thực thể IT bên ngoài tương tác với nó. Trong mọi trường hợp, TOE phải được cài đặt và quản trị theo các hướng dẫn cài đặt và quản trị TOE.

5.1.2 Chức năng an toàn được TOE cung cấp

Một hệ quản trị cơ sở dữ liệu được đánh giá dựa trên PP này sẽ cũng cấp các dịch vụ an toàn dưới đây.

Các dịch vụ an toàn được cung cấp bởi TOE:

- Kiểm soát truy cập tùy quyền DAC giới hạn truy cập tới đối tượng dựa trên định danh hoặc nhóm của chủ thể/đối tượng đó, và cho phép người dùng có thẩm quyền xác định cách bảo vệ *đối tượng*.
- Nắm bắt kiểm toán để tạo thông tin trên tất cả sự kiện có thể kiểm toán.
- Vai trò quản trị viên có thẩm quyền cho phép quản trị viên có thẩm quyền thiết lập chính sách kiểm soát truy cập tùy quyền, định danh và xác thực, và kiểm toán. TOE phải tuân thủ vai trò quản trị được ủy quyền.

CHÚ THÍCH: Một số quyền quản trị có thể gán cho người dùng cụ thể (thông qua việc gán quyền này họ trở thành những quản trị viên mặc dù chỉ có thể thực hiện một số hành động quản trị nhất định). TOE cung cấp chức năng an toàn để đảm bảo rằng người dùng không thể mở rộng quyền quản trị đã gán cho họ.

5.1.3 Chức năng an toàn tùy chọn

TOE hoặc môi trường công nghệ thông tin phải cung cấp dịch vụ an toàn.

Chức năng an toàn này không được mô tả trong các phần dưới đây của hồ sơ bảo vệ DBMS gói cơ sở. Tác giả ST phải kết hợp mô tả về chức năng an toàn bổ sung (tùy chọn) vào các yêu cầu chức năng an toàn tương ứng.

- Định danh và xác thực (I&A) theo đó người dùng được xác định duy nhất và được xác thực trước khi được ủy quyền truy cập thông tin được lưu trữ trên DBMS.
- Dịch vụ lưu trữ hồ sơ kiểm toán thực hiện lưu trữ hồ sơ tất cả các hoạt động liên quan đến an toàn mà người dùng thực hiện trên dữ liệu người dùng và DBMS.

- Dịch vụ soát xét kiểm toán cho phép quản trị viên có thẩm kiểm soát xét bản ghi kiểm toán đã lưu trữ để phát hiện việc vi phạm an toàn.

Tuy nhiên, việc tuân thủ tiêu chuẩn này không bảo đảm những nội dung sau:

- Cơ chế bảo vệ vật lý và thủ tục quản trị để sử dụng chúng đã được áp dụng.
- Các cơ chế đảm bảo tính sẵn có của dữ liệu nằm trên DBMS được đặt đúng chỗ. Dữ liệu trong DBMS có thể được truy cập bởi nhiều người tại một thời điểm nhất định. TOE có thể thực thi các giới hạn phân bổ tài nguyên của DBMS để ngăn chặn người dùng độc quyền sử dụng dịch vụ của DBMS. Tuy nhiên, nó không thể phát hiện hoặc ngăn chặn những lỗi liên quan đến tính sẵn sàng của dịch vụ, do thiên tai vật lý hoặc môi trường, sự cố thiết bị lưu trữ hoặc sự tấn công của tin tặc vào máy chủ vật lý. Đối với các mối đe dọa như vậy về tính sẵn sàng, môi trường phải cung cấp các biện pháp đối phó cần thiết.
- Các cơ chế để đảm bảo rằng người dùng bảo vệ đúng dữ liệu mà họ truy xuất từ DBMS được đặt đúng chỗ. Các thủ tục an toàn của (các) tổ chức sử dụng và quản lý DBMS phải xác định trách nhiệm của người dùng về truy xuất, lưu trữ, xuất dữ liệu và định vị.
- Cơ chế để đảm bảo rằng các quản trị viên có thẩm quyền sử dụng DAC một cách khôn ngoan. Mặc dù DBMS có thể hỗ trợ chính sách kiểm soát truy cập theo đó người dùng và tùy chọn người dùng trong các nhóm được xác định chỉ được phép truy cập vào dữ liệu mà họ cần để thực hiện công việc nhưng không thể đảm bảo hoàn toàn các quản trị viên có thẩm quyền có thể thiết lập kiểm soát truy cập rất thận trọng.

5.1.4 Môi trường vận hành TOE

5.1.4.1 Vùng bao

Thuật ngữ "vùng bao" (enclave) mô tả về môi trường trong đó TOE được thiết kế để hoạt động. Một vùng bao sẽ được kiểm soát bởi một cơ quan duy nhất và có một chính sách an toàn đồng nhất bao gồm: an toàn nhân sự và an toàn vật lý nhằm bảo vệ khỏi các môi trường khác. Một vùng bao đảm bảo bất kỳ yếu tố bên trong và bên ngoài nào truy cập vào tài nguyên trong khu vực đó phải đảm bảo chính sách của chính nó.

DBMS cũng có thể tương tác với các phần mềm có trên hệ điều hành máy chủ, môi trường vật lý của máy chủ và bên ngoài khu vực đó nhưng bên trong vùng bao. Cơ chế công nghệ thông tin và phi công nghệ thông tin được sử dụng để trao đổi thông tin an toàn giữa DBMS và các sản phẩm như vậy sẽ được xác định và điều phối bằng quản trị. Tương tự, các cơ chế công nghệ thông tin và phi công nghệ thông tin để đàm phán hoặc dịch các chính sách DAC tham gia vào các cuộc trao đổi như vậy sẽ được các tổ chức có liên quan giải quyết.

DBMS cũng có thể tương tác với các sản phẩm công nghệ thông tin bên ngoài vùng bao như là một cơ quan chứng thực (CA) được định nghĩa là một CA tin cậy bởi một sản phẩm công nghệ thông tin trong vùng bao này.

5.1.4.2 Kiến trúc TOE

Tiêu chuẩn này không chỉ định một kiến trúc cụ thể. Một TOE phù hợp với tiêu chuẩn này có thể được đánh giá và có thể hoạt động trong một số kiến trúc, bao gồm nhưng không giới hạn một hoặc nhiều các kiến trúc sau đây:

- Một hệ thống độc lập chạy ứng dụng máy chủ DBMS; một hệ thống độc lập chạy máy chủ DBMS và (các) máy khách DBMS và phục vụ một hoặc nhiều người sử dụng trực tuyến tại một thời điểm nhất định;
- Một mạng lưới các hệ thống giao tiếp với một số máy chủ DBMS phân tán đồng thời;
- Một mạng lưới các máy trạm hoặc các thiết bị đầu cuối chạy các máy khách DBMS và liên lạc đồng thời với một máy chủ DBMS; các thiết bị này có thể được nối tiếp đến máy chủ hoặc được kết nối với nó bằng các mạng cực bộ diện rộng;
- Một mạng máy trạm kết nối với một hoặc nhiều máy chủ ứng dụng, lần lượt tương tác với DBMS thay cho người dùng máy trạm hoặc các đối tượng khác (ví dụ: máy chủ DBMS tương tác với bộ xử lý giao dịch quản lý yêu cầu của người dùng);
- Một mạng lưới các máy trạm kết nối với một số máy chủ DBMS phân tán đồng thời; các máy chủ DBMS có thể nằm trong một mạng cục bộ duy nhất, hoặc chúng có thể được phân phối theo địa lý.

Tiêu chuẩn này cho phép hỗ trợ các kiến trúc khác nhau. Một kiến trúc có thể là một vùng bao, trong đó người dùng DBMS truy cập vào TOE thông qua một mạng nội bộ (LAN). Người dùng ở các vùng bao khác sẽ truy cập vào mạng LAN, máy chủ và máy chủ lưu trữ bằng một hoặc nhiều cơ chế bảo vệ ranh giới (ví dụ như một tường lửa) và sau đó thông qua một máy chủ truyền thông hoặc bộ định tuyến tới mạng LAN. Tùy thuộc vào cấu hình vùng bao cụ thể và chính sách truy cập DBMS mà nó hỗ trợ, tất cả người dùng (cả bên trong và bên ngoài vùng bao) sau đó có thể truy cập vào một máy chủ ứng dụng, kết nối người dùng TOE với máy tính vùng bao mà trên đó TOE điều hành hoặc quản lý phiên người dùng/DBMS hoàn chỉnh.

5.1.4.3 Quản trị TOE

Tiêu chuẩn này định nghĩa một vai trò quản trị viên cần thiết (quản trị viên có thẩm quyền) được thiết lập bởi nhà phát triển của DBMS. Tiêu chuẩn này cho phép nhà phát triển DBMS hoặc tác giả ST xác định nhiều vai trò hơn.

Nếu đích an toàn ST cho phép, các quản trị viên của hệ thống có thể gán các đặc quyền cho người dùng. Khi DBMS được thiết lập, khả năng phân quyền và trách nhiệm liên quan của nó cũng phải tồn tại. Các quản trị viên có thẩm quyền của TOE sẽ có các quyền hạn tương ứng với các đặc quyền được chỉ định. Tất nhiên, chính khả năng thiết lập và gán các đặc quyền sẽ là một chức năng đặc quyền.

5.2 Cấu hình PP

Hồ sơ bảo vệ cho hệ quản trị cơ sở dữ liệu (DBMS PP) được cấu trúc như là một hồ sơ bảo vệ cơ sở, có thể chứa một tập hợp các gói mở rộng hồ sơ bảo vệ (tùy chọn). Cấu trúc này được chọn để tối đa hóa khả năng thích ứng cho các môi trường hoạt động khác nhau và các yêu cầu hoạt động khác nhau, vì DBMS có thể cung cấp chức năng theo nhiều cách khác nhau. Các cấu hình PP sau đây được cho phép:

- Hồ sơ bảo vệ cho hệ quản trị cơ sở dữ liệu (Gói cơ sở) (DBMS PP);
- Hồ sơ bảo vệ cho hệ quản trị cơ sở dữ liệu (Gói cơ sở) DBMS PP với Gói mở rộng - Lịch sử Truy cập (DBMSPP-AH).

5.3 Quy ước

Tiêu chuẩn này cho phép một số thao tác đối với các yêu cầu chức năng: *tinh chỉnh, lựa chọn, chỉ định và lặp lại* được định nghĩa trong điều 8 của TCVN 8709-1:2011.

Thao tác **tinh chỉnh** được sử dụng để thêm chi tiết cho một yêu cầu và do đó hạn chế hơn nữa một yêu cầu. Việc tinh chỉnh các yêu cầu an toàn được biểu thị bằng văn bản in đậm hoặc trong trường hợp xóa, bằng cách ~~**gạch bỏ văn bản in đậm**~~.

Thao tác **lựa chọn** được sử dụng để chọn một hoặc nhiều tùy chọn do tiêu chuẩn cung cấp để nêu rõ yêu cầu. Các lựa chọn đã được thực hiện bởi các tác giả PP được biểu thị bằng *văn bản in nghiêng*, các lựa chọn được thực hiện bởi tác giả ST xuất hiện trong ngoặc vuông với dấu hiệu biểu thị lựa chọn sẽ được thực hiện, [lựa chọn:], và được *in nghiêng*.

Thao tác **chỉ định** được sử dụng để gán một giá trị cụ thể cho một tham số không xác định, chẳng hạn như độ dài của mật khẩu. Các chỉ định được thực hiện bởi các tác giả PP được biểu thị bằng cách hiển thị giá trị trong ngoặc vuông, [chỉ định_giá trị], các chỉ định được thực hiện bởi tác giả ST xuất hiện trong ngoặc vuông với dấu hiệu chỉ ra rằng phép chỉ định sẽ được thực hiện [chỉ định:] và được *in nghiêng*.

Thao tác **lặp lại** được sử dụng khi một thành phần được lặp lại với các hoạt động khác nhau. Lặp lại được biểu thị bằng cách hiển thị số lần lặp trong ngoặc đơn sau mã định danh thành phần, (số lần lặp).

6 Các tuyên bố tuân thủ

6.1 Các yêu cầu phù hợp CC

Tiêu chuẩn này phù hợp với TCVN 8709-2:2011 và TCVN 8709-3:2011.

6.2 Yêu cầu phù hợp với các gói

Tiêu chuẩn này quy định cấp đảm bảo đánh giá EAL2 tăng bởi ALC_FLR.2.

6.3 Yêu cầu phù hợp với các PP khác

Tiêu chuẩn này không yêu cầu tuân thủ bất kỳ hồ sơ bảo vệ nào khác.

6.4 Báo cáo phù hợp

Tiêu chuẩn này yêu cầu tuân thủ có thể diễn giải bởi một ST.

7 Mô tả các vấn đề an toàn

Phần này định nghĩa các vấn đề an toàn (SPD) của DBMS. Đầu tiên giới thiệu về các thảo luận không chính thức về SPD, sau đó là các mô tả chính thức hơn về các mối đe dọa đã xác định, các chính sách và các giả định và sẽ được sử dụng để xác định các yêu cầu an toàn cụ thể nêu tại tiêu chuẩn này.

7.1 Thảo luận không chính thức

Với việc sử dụng chung kho lưu trữ các dữ liệu giá trị cao, kẻ tấn công thường xuyên nhắm mục tiêu vào các cài đặt DBMS để gây tổn hại. Các lỗ hổng mà kẻ tấn công có thể lợi dụng là:

• Các lỗi thiết kế và lỗi lập trình trong DBMS và các chương trình, hệ thống liên quan, việc tạo các lỗ hổng an toàn khác nhau (ví dụ: các kiểm soát truy cập yếu hoặc không hiệu quả) có thể dẫn đến mất/sửa đổi dữ liệu, suy giảm hiệu suất...

• Hoạt động trái phép hoặc vô ý hoặc lạm dụng bởi người dùng cơ sở dữ liệu được ủy quyền hoặc người quản lý mạng/hệ thống hoặc bởi người dùng hoặc tin tặc trái phép (ví dụ: truy cập không phù hợp đối với dữ liệu nhạy cảm, siêu dữ liệu hoặc các chức năng trong cơ sở dữ liệu hoặc các thay đổi không phù hợp với chương trình cơ sở dữ liệu, cấu trúc hoặc cấu hình an toàn).

• Nhiễm phần mềm độc hại gây ra các sự cố như truy cập trái phép, rò rỉ hoặc tiết lộ dữ liệu cá nhân hoặc độc quyền, xóa hoặc làm hỏng dữ liệu hoặc chương trình, gián đoạn hoặc từ chối quyền truy cập vào cơ sở dữ liệu, các tấn công vào các hệ thống khác và các lỗi dịch vụ cơ sở dữ liệu không dự đoán được.

• Sửa đổi và/hoặc mất dữ liệu do nhập dữ liệu hoặc lệnh không hợp lệ, lỗi trong cơ sở dữ liệu hoặc quy trình quản trị hệ thống, phá hoại/thiệt hại hình sự...

7.2 Tài sản và các tác nhân đe dọa

Các mối đe dọa được đưa ra trong điều 7.3 đề cập đến các tài sản và tác nhân đe dọa khác nhau. Thuật ngữ "tác nhân đe dọa" là được định nghĩa trong TCVN 8709-1:2011. Thuật ngữ "người dùng hoặc quá trình thay mặt người dùng" được sử dụng trong PP này, chỉ định một loại thực thể cụ thể có thể tác động xấu đến tài sản.

Các tài sản, được đề cập trong Bảng 1 bên dưới được xác định trong TCVN 8709-1:2011 hoặc trong điều 3 "Thuật ngữ và định nghĩa".

Các thuật ngữ "dữ liệu TSF", "TSF" và "dữ liệu người dùng", được định nghĩa trong TCVN 8709-1:2011. Thuật ngữ "mã thực thi trong TSF "," đối tượng công cộng "," tài nguyên TOE "và" dữ liệu cấu hình" được đưa ra trong điều 3 "Thuật ngữ và định nghĩa".

7.3 Các mối đe dọa

Các mối đe dọa sau đây được xác định và giải quyết bởi TOE, và nên được đọc cùng với sở cứ trong điều 11.1.

TOE tuân thủ sẽ cung cấp chức năng an toàn nhằm giải quyết các mối đe dọa đối với TOE và thực hiện các chính sách được áp đặt bởi pháp luật hoặc quy định.

Bảng 1 - Các mối đe dọa áp dụng cho TOE

Mối đe dọa	Định nghĩa
T.ACCESS_TSFDATA	Một tác nhân đe dọa có thể đọc hoặc sửa đổi dữ liệu TSF bằng cách sử dụng các chức năng của TOE mà không có sự cho phép hợp lệ.
T.ACCESS_TSFFUNC	Một tác nhân đe dọa có thể sử dụng hoặc quản lý TSF, bỏ qua các cơ chế bảo vệ của TSF.
T.IA_MASQUERADE	Người dùng hoặc quy trình thay mặt cho người dùng có thể giả mạo một thực thể được ủy quyền để truy cập trái phép vào dữ liệu người dùng, dữ liệu TSF hoặc tài nguyên TOE.
T.IA_USER	Một tác nhân đe dọa có thể truy cập dữ liệu người dùng, dữ liệu TSF, hoặc tài nguyên TOE ngoại trừ các đối tượng công khai mà không được định danh và xác thực.
T.RESIDUAL_DATA	Một người dùng hoặc quy trình thay mặt cho người dùng có thể truy cập trái phép vào dữ liệu người dùng hoặc TSF thông qua việc phân bổ lại tài nguyên TOE từ một người dùng hoặc quy trình này sang người dùng khác hoặc quy trình khác.
T.TSF_COMPROMISE	Người dùng hoặc một quy trình thay mặt cho người dùng có thể khiến dữ liệu cấu hình bị truy cập trái phép (xem, sửa đổi hoặc xóa) hoặc có thể phá hoại mã thực thi trong TSF.
T.UNAUTHORIZED_ACCESS	Một tác nhân đe dọa có thể truy cập trái phép vào dữ liệu người dùng mà chúng không được ủy quyền theo chính sách an toàn TOE.

7.4 Chính sách an toàn của tổ chức

Các chính sách an toàn của tổ chức sau đây được giải quyết bằng các TOE phù hợp với PP:

Bảng 2 - Chính sách an toàn áp dụng cho TOE

Chính sách	Định nghĩa
P.ACCOUNTABILITY	Người dùng được ủy quyền của TOE sẽ phải chịu trách nhiệm về hành động của mình trong TOE.
P.ROLES	Vai trò giới hạn, được giao cho quản trị viên, phân tách và khác biệt với những quản trị viên khác.

P.USER	Cơ quan chỉ cấp quyền cho người dùng được tin tưởng để thực hiện các hành động xác định.

7.5 Các giả định

Phần này chứa các giả định liên quan đến môi trường CNTT nơi TOE sẽ cư trú.

Bảng 3 - Các giả định áp dụng cho môi trường TOE

Giả định	Định nghĩa
Về mặt vật lý	
A.PHYSICAL	Giả định rằng môi trường công nghệ thông tin cung cấp TOE với mức an toàn vật lý thích hợp, tương xứng với giá trị của tài sản công nghệ thông tin được bảo vệ bởi TOE.
Về mặt con người	
A.AUTHUSER	Giả định rằng người dùng được cấp quyền có những quyền truy cập cần thiết đủ để truy cập tối thiểu những thông tin do TOE quản lý.
A.MANAGE	Giả định rằng chức năng an toàn TOE được quản lý bởi một hoặc nhiều quản trị viên có thẩm quyền. Quản trị viên của hệ thống không phải là người bất cẩn, cố tình lơ là hoặc có thái độ thù địch, sẽ tuân theo và tuân thủ đầy đủ các yêu cầu được cung cấp bởi tài liệu hướng dẫn.
A.TRAINEDUSER	Giả định rằng người dùng được đào tạo đầy đủ và đáng tin cậy để hoàn thành một số tác vụ hoặc nhóm tác vụ trong môi trường công nghệ thông tin an toàn bằng cách thực hiện kiểm soát hoàn toàn dữ liệu người dùng của họ.
Về mặt quy trình	
A.NO_GENERAL_ PURPOSE	Không có các thành phần có khả năng tính toán chung (ví dụ, trình biên dịch hoặc các ứng dụng người dùng) có sẵn trên các máy chủ hệ quản trị cơ sở dữ liệu, ngoài các dịch vụ cần thiết cho hoạt động, quản trị và hỗ trợ của hệ quản trị cơ sở dữ liệu.
A.PEER_FUNC_&_ MGT	Tất cả các hệ thống công nghệ thông tin đáng tin cậy từ xa được tin tưởng bởi TSF để cung cấp dữ liệu hoặc dịch vụ TSF cho TOE, hoặc để hỗ trợ TSF trong việc thực thi các quyết định chính sách an toàn được giả định thực hiện chính xác các chức năng được TSF sử dụng, phù hợp với các giả định được xác định cho chức năng này và được quản lý, vận hành hợp lý theo các ràng buộc về chính sách an toàn tương thích với các yêu cầu an toàn của TOE.
A.SUPPORT	Bất kỳ thông tin nào được cung cấp bởi một thực thể đáng tin cậy

	trong môi trường công nghệ thông tin và được sử dụng để hỗ trợ xác thực và ủy quyền của người dung được sử dụng bởi TOE là chính xác và cập nhật.
Về mặt kết nối	
A.CONNECT	Tất cả các kết nối đến và đi từ các hệ thống công nghệ đáng tin cậy từ xa và giữa các phần riêng biệt của TSF được bảo vệ về mặt vật lý hoặc logic trong môi trường TOE để đảm bảo tính toàn vẹn và an toàn của dữ liệu được truyền đi và để đảm bảo tính xác thực của các điểm đầu cuối. Chú thích áp dụng: Nếu TOE bao gồm các phần riêng biệt và TOE thực hiện cơ chế đảm bảo bảo vệ dữ liệu TSF chuyển qua giữa các phần này, tác giả ST có thể xem xét yêu cầu FPT_ITT.1 để bổ sung hoặc thay thế A.CONNECT.

8 Các mục tiêu an toàn

Phần này xác định các mục tiêu an toàn của TOE và môi trường hỗ trợ của nó.

Các mục tiêu an toàn xác định trách nhiệm của TOE và môi trường của nó trong việc đáp ứng định nghĩa các vấn đề an toàn (SPD).

8.1 Các mục tiêu an toàn cho TOE

Bảng 4 - Mục tiêu an toàn TOE

Mục tiêu	Định nghĩa mục tiêu
O.ADMIN_ROLE	TOE sẽ cung cấp một cơ chế (ví dụ: một "vai trò") mà theo đó các hành động sử dụng đặc quyền quản trị có thể bị hạn chế.
O.AUDIT_GENERATION	TSF phải có khả năng ghi lại các sự kiện liên quan đến an toàn được xác định (thường bao gồm các hành động quan trọng về an toàn của người dùng TOE). Thông tin ghi lại cho các sự kiện liên quan đến an toàn phải bao gồm thời gian và ngày tháng xảy ra sự kiện và, nếu có thể, xác định người dùng gây ra sự kiện và phải đủ chi tiết để giúp người dùng được ủy quyền phát hiện các vi phạm an toàn hoặc xác định cấu hình sai của các tính năng an toàn TOE mà để cho các tài sản công nghệ thông tin mở ra và hư hại.
O.DISCRETIONARY_ACCESS	TSF phải kiểm soát được việc truy cập của các đối tượng và/hoặc người dùng vào các tài nguyên được đặt tên dựa trên định danh chủ thể, đối tượng hoặc người sử dụng. TSF phải cho phép người dùng được ủy quyền được chỉ định cho mỗi chế độ truy cập mà người dùng/đối tượng được phép truy cập vào một đối tượng được đặt tên

	cụ thể trong chế độ truy cập đó.
O.I&A	TOE phải đảm bảo rằng người dùng đã được xác thực trước khi TOE xử lý bất kỳ hành động nào cần xác thực.
O.MANAGE	TSF phải cung cấp tất cả các chức năng và phương tiện cần thiết để hỗ trợ người dùng được ủy quyền chịu trách nhiệm quản lý các cơ chế an toàn TOE, phải cho phép hạn chế các hành động quản lý như vậy đối với những người dùng riêng biệt và phải đảm bảo rằng chỉ có những người dùng được ủy quyền đó mới có thể truy cập các chức năng quản lý.
O.MEDIATE	TOE phải bảo vệ dữ liệu người dùng theo chính sách an toàn của nó và phải điều đình tất cả yêu cầu truy cập dữ liệu đó.
O.RESIDUAL_INFORMATION	TOE sẽ đảm bảo rằng bất kỳ thông tin nào chứa trong một tài nguyên được bảo vệ trong phạm vi kiểm soát của nó sẽ được chia sẻ chính xác khi phân bổ lại các tài nguyên này.
O.TOE_ACCESS	TOE sẽ cung cấp các chức năng kiểm soát truy cập logic của người dùng vào dữ liệu người dùng và TSF.

8.2 Các mục tiêu an toàn trong môi trường hoạt động

Bảng 5 – Các mục tiêu an toàn trong môi trường hoạt động

Mục tiêu	**Mô tả mục tiêu**
OE.ADMIN	Những người chịu trách nhiệm về TOE là những cá nhân có thẩm quyền và đáng tin cậy, có khả năng quản lý TOE và an toàn thông tin trong nó.
OE.INFO_PROTECT	Những người chịu trách nhiệm về TOE phải thiết lập và thực hiện các thủ tục để đảm bảo rằng thông tin được bảo vệ một cách thích hợp. Cụ thể: Tất cả các mạng và cáp ngoại vi phải được phê duyệt để các dữ liệu nhạy cảm nhất được truyền qua. Các liên kết vật lý này được giả định là được bảo vệ đầy đủ để chống lại các mối đe dọa đối với tính bí mật và tính toàn vẹn của dữ liệu bằng các kỹ thuật bảo vệ logic và vật lý thích hợp. Việc bảo vệ DAC trên các tệp tin có liên quan đến an toàn (chẳng hạn như các dấu vết kiểm toán và cơ sở dữ liệu ủy quyền) luôn được thiết lập chính xác. Người dùng được phép truy cập vào các phần của dữ liệu được quản

	lý bởi TOE và được đào tạo để kiểm soát dữ liệu của chính họ.
OE.NO_GENERAL_ PURPOSE	Không có các thành phần có khả năng tính toán chung (ví dụ, trình biên dịch hoặc các ứng dụng người dùng) có sẵn trên các máy chủ hệ quản trị cơ sở dữ liệu, ngoài các dịch vụ cần thiết cho hoạt động, quản trị và hỗ trợ của hệ quản trị cơ sở dữ liệu.
OE.PHYSICAL	Những người chịu trách nhiệm về TOE phải đảm bảo rằng những thành phần của TOE quan trọng đối với việc thực thi chính sách an toàn được bảo vệ khỏi các cuộc tấn công vật lý có thể ảnh hưởng đến các mục tiêu an toàn công nghệ thông tin. Việc bảo vệ phải tương xứng với giá trị của các tài sản công nghệ thông tin được bảo vệ bởi TOE.

Bảng 6 - Các mục tiêu an toàn trong môi trường hoạt động công nghệ thông tin

Mục tiêu	Mô tả mục tiêu
OE.IT_I&A	Bất kỳ thông tin nào được cung cấp bởi một thực thể đáng tin cậy trong môi trường và được sử dụng để hỗ trợ xác thực người dùng và ủy quyền được sử dụng bởi TOE là chính xác và được cập nhật.
OE.IT_REMOTE	Nếu TOE dựa vào các hệ thống công nghệ thông tin đáng tin cậy được điều khiển từ xa để hỗ trợ thực thi chính sách của mình, các hệ thống này phải đảm bảo các chức năng và dữ liệu được sử dụng bởi TOE trong việc đưa ra quyết định chính sách, và được yêu cầu bởi TOE phải được bảo vệ khỏi mọi cuộc tấn công dẫn tới sai lệch kết quả.
OE.IT_TRUSTED_SYSTEM	Các hệ thống công nghệ thông tin đáng tin cậy từ xa thực hiện các giao thức và cơ chế yêu cầu của TSF để hỗ trợ thực thi chính sách an toàn. Các hệ thống công nghệ thông tin đáng tin cậy từ xa này được quản lý theo các chính sách đã biết, được chấp nhận và đáng tin cậy dựa trên các quy tắc và chính sách tương tự áp dụng cho TOE và được bảo vệ về mặt vật lý và logic tương đương với TOE.

9 Yêu cầu chức năng an toàn mở rộng

FIA_USB_ (EXT).2 Ràng buộc người dùng-chủ thể nâng cao

FIA_USB_ (EXT).2 tương tự FIA_USB.1 ngoại trừ việc thêm khả năng chỉ định quy tắc theo đó các thuộc tính an toàn chủ thể cũng được lấy từ dữ liệu TSF ngoài thuộc tính an toàn người dùng.

Phân cấp thành phần

FIA_USB_ (EXT).2 được phân cấp theo FIA_USB.1.

Quản lý

Xem mô tả quản lý được chỉ định cho FIA_USB.1 trong TCVN 8709.

Kiểm toán

Xem yêu cầu kiểm toán được chỉ định cho FIA_USB.1 trong TCVN 8709

FIA_USB_ (EXT).2 Ràng buộc người dùng–chủ thể nâng cao

Phân cấp theo: FIA_USB.1 Ràng buộc người dùng–chủ thể

Phụ thuộc: FIA_ATD.1 Định nghĩa thuộc tính người dùng

FIA_USB_ (EXT).2.1

TSF sẽ liên kết các thuộc tính an toàn người dùng sau với các chủ thể hoạt động thay mặt người dùng đó: [chỉ định: danh sách các thuộc tính an toàn người dùng].

FIA_USB_ (EXT).2.2

TSF sẽ thực thi các quy tắc sau đây về sự liên kết ban đầu của thuộc tính an toàn người dùng với các chủ thể thay mặt người dùng: [chỉ định: quy tắc cho sự liên kết ban đầu của các thuộc tính].

FIA_USB_ (EXT).2.3

TSF sẽ thực thi các quy tắc sau đây chi phối các thay đổi đối với các thuộc tính an toàn người dùng được liên kết với các chủ thể thay mặt người dùng: [chỉ định: quy tắc cho việc thay đổi thuộc tính].

FIA_USB_ (EXT).2.4

TSF sẽ thực thi các quy tắc sau đây để chỉ định thuộc tính an toàn chủ thể không xuất phát từ thuộc tính an toàn người dùng khi một chủ thể được tạo: [chỉ định: quy tắc cho liên kết ban đầu của an toàn chủ thể thuộc tính không xuất phát từ thuộc tính an toàn người dùng].

10 Các yêu cầu an toàn

10.1 Các yêu cầu chức năng an toàn

Phần này định nghĩa các yêu cầu chức năng cho TOE. Yêu cầu chức năng trong PP này được rút ra trực tiếp từ TCVN 8709-2:2011 hoặc dựa trên TCVN 8709-2:2011, bao gồm cả sử dụng các thành phần mở rộng. Những yêu cầu này có liên quan đến việc hỗ trợ hoạt động an toàn của TOE.

Bảng 7 - Các yêu cầu chức năng an toàn

Các thành phần chức năng	
FAU_GEN.1	Tạo dữ liệu kiểm toán.
FAU_GEN.2	Liên kết định danh người dùng.
FAU_SEL.1	Kiểm toán chọn lọc.
FDP_ACC.1	Kiểm soát truy cập trực tiếp.
FDP_ACF.1	Kiểm soát truy cập dựa trên thuộc tính an toàn.
FDP_RIP.1	Bảo vệ các thông tin còn lại.
FIA_ATD.1	Định nghĩa thuộc tính người dùng.
FIA_UAU.1	Thời gian xác thực.
FIA_UID.1	Thời gian định danh.
FIA_USB_(EXT).2	Tăng cường liên kết người dùng.
FMT_MOF.1	Quản lý hoạt động các chức năng an toàn.
FMT_MSA.1	Quản lý thuộc tính an toàn.
FMT_MSA.3	Khởi tạo thuộc tính tĩnh.
FMT_MTD.1	Quản lý dữ liệu TSF.
FMT_REV.1(1)	Thu hồi (thuộc tính người dùng).
FMT_REV.1(2)	Thu hồi (tiêu đề, thuộc tính đối tượng).
FMT_SMF.1	Xác định chức năng an toàn.
FMT_SMR.1	Các vai trò an toàn.
FPT_TRC.1	TSF nội bộ.
FTA_MCS.1	Giới hạn cơ bản về nhiều phiên đồng thời.
FTA_TSE.1	Thiết lập phiên TOE.

10.1.1 Kiểm toán an toàn (FAU)

10.1.1.1 FAU_GEN.1 Tạo dữ liệu kiểm toán

FAU_GEN.1.1

TSF phải tạo bản ghi kiểm toán gồm các sự kiện kiểm toán sau:

a) Bật và tắt chức năng kiểm toán;

b) Tất cả các sự kiện có thể kiểm toán với mức kiểm toán tối thiểu liệt kê trong Bảng 7: Sự kiện có thể kiểm toán;

c) Bật và tắt DBMS;

d) Sử dụng quyền đặc biệt (ví dụ quản trị viên có thẩm quyền thay đổi chính sách kiểm soát truy cập);

e) [lựa chọn: *[chỉ định: sự kiện ở mức kiểm toán tối thiểu nêu trong SFR bổ sung mà tác giả ST đưa ra],* [chỉ định: *sự kiện tương ứng với mức kiểm toán tối thiểu nêu trong các yêu cầu mở rộng mà tác giả ST đưa ra], "không có sự kiện nào khác"]].*

Chú thích áp dụng 1: Với lựa chọn, tác giả ST phải chọn một hoặc tất cả chỉ định (như nêu chi tiết trong đoạn sau) hoặc lựa chọn "không có sự kiện nào khác".

Chú thích áp dụng 2: Với chỉ định đầu tiên, tác giả ST phải bổ sung bảng (hoặc danh sách rõ ràng) sự kiện kiểm toán kết hợp với mức kiểm toán tối thiểu với tất cả SFR mà tác giả ST đưa ra không nằm trong tiêu chuẩn này.

Chú thích áp dụng 3: Tương tự như vậy, nếu tác giả ST đưa ra các yêu cầu mở rộng không có trong tiêu chuẩn này thì các sự kiện kiểm toán tương ứng phải được thêm vào tại chỉ định thứ 2. Vì các yêu cầu không định nghĩa kiểm toán "tối thiểu", nên tác giả ST phải xác định tập sự kiện tương ứng với loại thông tin được kiểm toán ở mức tối thiểu với các yêu cầu giống nhau.

Chú thích áp dụng 4: Nếu không có SFR bổ sung (TCVN 8709 hoặc mở rộng) hoặc SFR bổ sung không có kiểm toán tối thiểu thì có thể chấp nhận chỉ định "không có sự kiện nào khác" trong phần này.

FAU_GEN.1.2

TSF phải tạo bản ghi kiểm toán gồm các sự kiện kiểm toán sau:

- Ngày và thời gian sự kiện, loại sự kiện, định danh tiêu đề (nếu áp dụng) và kết quả sự kiện (thành công hay thất bại);
- Với mỗi loại sự kiện kiểm toán, dựa trên định nghĩa sự kiện có thể kiểm toán của các thành phần chức năng trong PP/ST này, [thông tin trong cột thứ 3 bảng 8: Sự kiện có thể kiểm toán].

Chú thích áp dụng: Trong cột 3 của bảng dưới đây, "Nội dung bản ghi kiểm toán bổ sung" được sử dụng để xác định dữ liệu phải có trong bản ghi kiểm toán nếu nó nằm trong phạm vi sự kiện tạo ra bản ghi. Nếu không yêu cầu thông tin nào (ngoài những thông tin đã liệt kê trong điểm a ở trên) cho loại sự kiện có thể kiểm toán thì có thể chấp nhận chỉ định "Không có".

Bảng 8 - Sự kiện có thể kiểm toán

Yêu cầu chức năng an toàn	**Sự kiện có thể kiểm toán**	**Nội dung bản ghi kiểm toán bổ sung**
FAU_GEN.1	Không có.	Không có.

FAU_GEN.2	Không có.	Không có.
FAU_SEL.1	Tất cả sửa đổi cấu hình kiểm toán xảy ra trong chức năng thu thập kiểm toán đang hoạt động.	Định danh quản trị viên có thẩm quyền làm thay đổi cấu hình kiểm toán.
FDP_ACC.1	Không có.	Không có.
FDP_ACF.1	Các yêu cầu thực hiện một hoạt động trên một đối tượng SFP đã chỉ ra thành công.	Định danh chủ thể thực hiện hành động.
FDP_RIP.1	Không có.	Không có.
FIA_ATD.1	Không có.	Không có.
FIA_UAU.1	Sử dụng cơ chế xác thực không thành công	Không có.
FIA_UID.1	Sử dụng cơ chế xác thực không thành công.	Không có.
FIA_USB_ (EXT).2	Sử dụng cơ chế định danh người dùng không thành công, bao gồm định danh người dùng đã cấp.	Không có.
FMT_MOF.1	Không có.	Không có.
FMT_MSA.1	Không có.	Không có.
FMT_MSA.3	Không có.	Không có.
FMT_MTD.1	Không có.	Không có.
FMT_REV.1(1)	Thu hồi thuộc tính an toàn không thành công.	Định danh thành phần cố gắng thu hồi thuộc tính an toàn.
FMT_REV.1(2)	Thu hồi thuộc tính an toàn không thành công.	Định danh thành phần cố gắng thu hồi thuộc tính an toàn.
FMT_SMF.1	Sử dụng của các chức năng quản lý.	Định danh quản trị viên đang thực hiện các chức năng.
FMT_SMR.1	Việc thay đổi vai trò của nhóm người dùng	Định danh quản trị viên có thẩm quyền thay đổi định nghĩa vai trò.
FPT_TRC.1	Khôi phục tính nhất quán.	Không có.
FTA_MCS.1	Từ chối phiên mới dựa trên giới hạn các phiên đồng thời.	Không có.
FTA_TSE.1	Từ chối thiết lập phiên tùy thuộc vào cơ chế thiết lập phiên.	Định danh của thành phần cố gắng thiết lập phiên.

10.1.1.2 FAU_GEN.2 Liên kết định danh người dùng

FAU_GEN.2.1

Đối với các sự kiện kiểm toán phát sinh từ hành động của người dùng đã được định danh **và bất kỳ nhóm nào đã được định danh**, TSF sẽ có thể liên kết mỗi sự kiện có thể kiểm toán với định danh của [lựa chọn: "*người dùng*", *"người dùng **và nhóm**"]* gây ra sự kiện.

10.1.1.3 FAU_SEL.1 Kiểm toán chọn lọc

FAU_SEL.1.1

TSF sẽ có thể chọn bộ sự kiện được kiểm toán từ tập hợp của tất cả các sự kiện có thể kiểm toán dựa trên các thuộc tính sau:

a) *Định danh đối tượng;*

b) *Định danh người dùng;*

c) [lựa chọn: "*định danh chủ thể*", *"định danh máy chủ"*, ***"định danh nhóm", "không có các định danh khác"];***

d) *Loại sự kiện;*

e) [Sự thành công của các sự kiện an toàn có thể kiểm toán];

f) Sự thất bại của các sự kiện an toàn có thể kiểm toán;

g) [Lựa chọn: [chỉ định: *danh sách các thuộc tính bổ sung mà dựa vào đó để chọn lọc kiểm toán*]].

Chú thích áp dụng 1: "loại sự kiện" được xác định bởi tác giả ST; mục đích là để có thể bao gồm hoặc loại trừ các lớp sự kiện kiểm toán.

Chú thích áp dụng 2: Mục đích của yêu cầu này là thu thập đủ dữ liệu kiểm toán để cho phép các quản trị viên thực hiện nhiệm vụ của họ, không nhất thiết chỉ nắm bắt các dữ liệu kiểm toán cần thiết. Nói cách khác, DBMS không nhất thiết phải bao gồm hoặc loại trừ các sự kiện có thể kiểm toán dựa trên tất cả các thuộc tính tại bất kỳ thời điểm nào.

10.1.2 Bảo vệ dữ liệu người dùng (FDP)

10.1.2.1 FDP_ACC.1 Kiểm soát truy cập trực tiếp

FDP_ACC.1.1

TSF sẽ thực thi [chính sách kiểm soát truy cập tùy quyền] đối với các đối tượng trên [tất cả các đối tượng, tất cả các đối tượng được kiểm soát bởi DBMS, và tất cả các hoạt động trong số đó].

10.1.2.2 FDP_ACF.1 Kiểm soát truy cập dựa trên thuộc tính an toàn

FDP_ACF.1.1

TSF sẽ thực thi [chính sách kiểm soát truy cập tùy quyền] đối với các đối tượng dựa trên: [chỉ định: danh sách các đối tượng và đối tượng được kiểm soát theo SFP được chỉ định và đối với mỗi thuộc tính an toàn có liên quan SFP hoặc các nhóm có liên quan của SFP có liên quan thuộc tính an toàn].

Chú thích áp dụng: Đối tượng được kiểm soát bởi DBMS có thể là các đối tượng thực hiện cụ thể được trình bày cho người dùng được ủy quyền tại giao diện người dùng cho DBMS. Chúng có thể bao gồm, nhưng không giới hạn ở các bảng biểu, hồ sơ, tệp, chỉ mục, chế độ xem, ràng buộc, truy vấn được lưu trữ và dữ liệu đặc tả. Cấu trúc dữ liệu không được trình bày cho người dùng được ủy quyền ở giao diện người dùng DBMS, nhưng được sử dụng nội bộ, là các cấu trúc dữ liệu nội bộ TSF. Cấu trúc dữ liệu nội bộ TSF không được kiểm soát theo các quy tắc được chỉ định trong FDP_ACF.1.

FDP_ACF.1.2

TSF sẽ thực thi các quy tắc sau để xác định xem các hành động giữa các chủ thể và đối tượng được cho phép hay không: [chỉ định: *các quy tắc điều chỉnh quyền truy cập giữa các chủ thể và các đối tượng được kiểm soát sử dụng các hoạt động có kiểm soát đối với các đối tượng bị kiểm soát*].

FDP_ACF.1.3

TSF sẽ cấp phép quyền truy cập cho các chủ thể vào các đối tượng một cách rõ ràng dựa trên các quy tắc bổ sung sau đây: [chỉ định: *các quy tắc, dựa trên các thuộc tính an toàn, sẽ cấp phép truy cập cho các chủ thể vào các đối tượng một cách rõ ràng*].

FDP_ACF.1.4

TSF sẽ từ chối rõ ràng việc truy cập các chủ thể vào các đối tượng dựa trên các quy tắc bổ sung sau: [chỉ định: *các quy tắc, dựa trên các thuộc tính an toàn, cho phép rõ ràng quyền truy cập các chủ thể vào các đối tượng*].

10.1.2.3 FDP_RIP.1 Bảo vệ các thông tin còn lại

FDP_RIP.1.1

TSF sẽ đảm bảo rằng bất kỳ nội dung thông tin trước đây nào của một tài nguyên không được thực hiện khi *phân bổ tài nguyên* cho các đối tượng sau: [chỉ định: *danh sách các đối tượng*].

10.1.3 Định danh và xác thực (FIA)

Chú thích áp dụng: Tác giả ST cần lưu ý họ định danh và xác thực được viết theo cách mà các SFR có thể được sử dụng trong trường hợp các dịch vụ định danh và xác thực được thực hiện bởi chính TOE hoặc được thực hiện trong môi trường TOE.

10.1.3.1 FIA_ATD.1 Định nghĩa thuộc tính người dùng

FIA_ATD.1.1

TSF sẽ duy trì danh sách các thuộc tính an toàn sau đây của người dùng cá nhân:

a) [Định danh người dùng cơ sở dữ liệu và bất kỳ thành viên nhóm liên kết nào;

b) Các vai trò cơ sở dữ liệu liên quan đến an toàn;

c) [Chỉ định: danh sách các thuộc tính an toàn]].

Chú thích áp dụng: Mục đích của yêu cầu này là xác định các thuộc tính an toàn TOE mà TOE sử dụng để xác định quyền truy cập. Những thuộc tính này có thể được kiểm soát bởi môi trường hoặc bởi chính TOE.

10.1.3.2 FIA_UAU.1 Thời gian xác thực

FIA_UAU.1.1

TSF sẽ cho phép [chỉ định: *danh sách các hành động trung gian TSF*] được thực hiện thay mặt người dùng trước khi người dùng được xác thực.

FIA_UAU.1.2

TSF sẽ yêu cầu mỗi người dùng phải được xác thực thành công trước khi cho phép thực hiện bất kỳ hành động trung gian TSF thay mặt người dùng đó.

10.1.3.3 FIA_UID.1 Thời gian định danh

FIA_UID.1.1

TSF sẽ cho phép [chỉ định: *danh sách các hành động trung gian TSF*] được thực hiện thay mặt người dùng trước khi người dùng được định danh.

FIA_UID.1.2

TSF sẽ yêu cầu mỗi người dùng được định danh thành công trước khi cho phép thực hiện bất kỳ hành động trung gian TSF thay mặt người dùng đó.

10.1.3.4 FIA_USB_(EXT).2 Tăng cường liên kết người dùng-chủ thể

FIA_USB_ (EXT).2.1

TSF sẽ kết hợp các thuộc tính an toàn người dùng sau với các chủ thể hoạt động thay mặt cho người dùng đó: [chỉ định: *danh sách các thuộc tính an toàn*].

FIA_USB_ (EXT).2.2

TSF sẽ thực thi các quy tắc sau về mối liên kết ban đầu của các thuộc tính an toàn người dùng với các chủ thể hoạt động thay mặt cho người dùng: [chỉ định: *quy tắc cho mối liên kết ban đầu của các thuộc tính*].

FIA_USB_ (EXT).2.3

TSF sẽ thực thi các quy tắc sau điều chỉnh thay đổi đối với các thuộc tính an toàn của người dùng liên quan đến các chủ thể hoạt động thay mặt cho người dùng: [chỉ định: *các quy tắc để thay đổi các thuộc tính*].

FIA_USB_ (EXT).2.4

TSF sẽ thực thi các quy tắc sau để phân định các thuộc tính an toàn theo chủ thể không bắt nguồn từ các thuộc tính an toàn của người dùng khi tạo đối tượng: [chỉ định: *các quy tắc cho mối liên kết ban đầu của các thuộc tính an toàn đối tượng không bắt nguồn từ các thuộc tính an toàn của người dùng*].

10.1.4 Quản lý an toàn (FMT)

10.1.4.1 FMT_MOF.1 Quản lý an toàn các chức năng theo hành vi

FMT_MOF.1.1

TSF sẽ hạn chế khả năng *vô hiệu hóa và kích hoạt* các chức năng [liên quan đến các đặc tả của các sự kiện được kiểm toán] cho [quản trị viên có thẩm quyền].

10.1.4.2 FMT_MSA.2 Quản lý các thuộc tính an toàn

FMT_MSA.1.1

TSF sẽ thực thi [kiểm soát truy cập tùy quyền] để hạn chế khả năng quản lý [tất cả] các thuộc tính an toàn cho [quản trị viên có thẩm quyền].

Chú thích áp dụng: Tác giả ST phải đảm bảo rằng tất cả các thuộc tính được xác định trong FIA_ATD.1 được quản lý và bảo vệ đầy đủ.

10.1.4.3 FMT_MSA.3 Khởi tạo thuộc tính tĩnh

FMT_MSA.3.1

TSF sẽ thực thi [kiểm soát truy cập tùy quyền] để cung cấp các giá trị mặc định hạn chế cho các thuộc tính an toàn được sử dụng để thi hành SFP.

Chú thích áp dụng: Yêu cầu này áp dụng cho các đối tượng mới ở cấp cao nhất (ví dụ: các bảng). Khi các đối tượng cấp thấp hơn được tạo ra (ví dụ: các hàng, ô), mặc định chúng có thể kế thừa các quyền của các đối tượng cấp cao nhất. Nói cách khác, các quyền của các đối tượng "con" có thể nhận các quyền của đối tượng "cha" theo mặc định.

FMT_MSA.3.2

TSF sẽ cho phép [không có người dùng] chỉ định các giá trị ban đầu thay thế để ghi đè các giá trị mặc định khi một đối tượng hoặc thông tin được tạo ra.

10.1.4.4 FMT_MTD.1 Quản lý dữ liệu TSF

FMT_MTD.1.1

TSF sẽ hạn chế khả năng *bao gồm hoặc loại trừ* [chỉ định: *các sự kiện có thể kiểm toán*] cho [quản trị viên có thẩm quyền].

10.1.4.5 FMT_REV.1 (1) Thu hồi

FMT_REV.1.1 (1)

TSF sẽ hạn chế khả năng thu hồi [chỉ định: *danh sách các thuộc tính an toàn*] liên kết với *người dùng* dưới sự kiểm soát của TSF cho [quản trị viên có thẩm quyền].

FMT_REV.1.2 (1)

TSF sẽ thực thi các quy tắc [chỉ định: *xác định các quy tắc thu hồi*].

10.1.4.6 FMT_REV.1 (2) Thu hồi

FMT_REV.1.1 (2)

TSF sẽ hạn chế khả năng thu hồi [chỉ định: *danh sách các thuộc tính an toàn*] kết hợp với *các đối tượng* thuộc quyền kiểm soát của TSF cho [quản trị viên được ủy quyền] **và người dùng cơ sở dữ liệu có đủ các đặc quyền như được cho phép theo chính sách kiểm soát truy cập tùy quyền**.

FMT_REV.1.2 (2)

TSF sẽ thực thi các quy tắc [chỉ định: cụ thể các quy tắc thu hồi].

10.1.4.7 FMT_SMF.1 Đặc điểm kỹ thuật của các chức năng quản lý

FMT_SMF.1.1

TSF sẽ có khả năng thực hiện các chức năng quản lý an toàn sau: [chỉ định: *danh sách các chức năng quản lý an toàn được cung cấp bởi TSF*].

10.1.4.8 FMT_SMR.1 Vai trò an toàn

FMT_SMR.1.1

TSF sẽ duy trì vai trò [quản trị viên có thẩm quyền và [chỉ định: *các vai trò được xác định bổ sung có thẩm quyền*]].

FMT_SMR.1.2

TSF sẽ có thể liên kết người dùng với vai trò.

Chú thích áp dụng: Yêu cầu này xác lập một bộ những vai trò tối thiểu của quản trị viên. ST hoặc môi trường vận hành có thể chứa các vai trò được phân tách mịn hơn tương ứng với các vai trò được xác định ở đây (ví dụ: người sử dụng không quản trị cơ sở dữ liệu hoặc người vận hành cơ sở dữ liệu). Tác giả ST có thể thay đổi tên của các vai trò được xác định ở trên nhưng vai trò "mới" vẫn phải thực hiện các chức năng mà các yêu cầu FMT trong tiêu chuẩn này đã xác định.

10.1.5 Bảo vệ của TSF (FPT)

Chú thích áp dụng: Ranh giới miền an toàn trong phần tử đầu tiên là miền TSF và mục đích của nó là bảo vệ TSF khỏi các đối tượng không tin cậy ở TSFI. Ranh giới miền an toàn trong phần tử thứ hai bao gồm toàn bộ phạm vi kiểm soát TOE và mục đích của nó là duy trì sự tách biệt giữa bất kỳ đối tượng nào trong phạm vi mà kiểm soát TOE.

10.1.5.1 FPT_TRC.1 Tính nhất quán bên trong TSF

FPT_TRC.1.1

TSF sẽ đảm bảo rằng dữ liệu TSF là nhất quán khi sao chép giữa các phần của TOE.

FPT_TRC.1.2

Khi các phần của TOE chứa dữ liệu TSF được sao chép lại, TSF sẽ đảm bảo tính nhất quán của dữ liệu TSF được sao chép khi kết nối lại trước khi xử lý bất kỳ yêu cầu nào cho [chỉ định: *danh sách các chức năng phụ thuộc vào tính nhất quán sao chép dữ liệu TSF*].

Chú thích áp dụng: Yêu cầu này được đáp ứng không đáng kể nếu TOE không chứa các thành phần riêng biệt. Lưu ý: Thông thường, chúng ta không thể đạt được sự nhất quán hoàn toàn, liên tục của dữ liệu TSF được phân phối đến các phần từ xa của TOE vì các phần phân phối của TSF có thể hoạt động ở các thời điểm khác nhau hoặc bị ngắt kết nối với nhau. Yêu cầu này cố gắng giải quyết tình huống này một cách thực tế bằng cách thừa nhận rằng sẽ có sự không nhất quán dữ liệu TSF nhưng chúng sẽ được sửa chữa kịp thời. Ví dụ, một TSF có thể cung cấp độ nhất quán kịp thời thông qua phát định kỳ dữ liệu TSF tới tất cả các nút TSF đang duy trì dữ liệu TSF được sao chép. Một ví dụ khác là TSF cung cấp một cơ chế thăm dò các nút TSF từ xa một cách rõ ràng cho sự không nhất quán và phản ứng với hành động để sửa chữa các sự không nhất quán được xác định.

10.1.6 Truy cập TOE (FTA)

10.1.6.1 FTA_MCS.1 Giới hạn cơ bản về nhiều phiên đồng thời

FTA_MCS.1.1

TSF sẽ hạn chế số phiên đồng thời tối đa thuộc cùng một người dùng.

FTA_MCS.1.2

TSF sẽ bắt buộc, theo mặc định, một giới hạn [chỉ định: *số mặc định*] phiên cho mỗi người dùng.

Chú thích áp dụng: Tác giả ST được nhắc nhở rằng TCVN 8709-2:2011 cho phép số mặc định có thể được định nghĩa là một chức năng quản lý trong FMT.

10.1.6.2 FTA_TSE.1 Thiết lập phiên TOE

FTA_TSE.1.1

> TSF sẽ có thể từ chối thiết lập phiên dựa trên [chỉ định: các thuộc tính có thể được đặt rõ ràng bởi (các) quản trị viên có thẩm quyền, bao gồm định danh người dùng và [lựa chọn: định danh nhóm, thời gian trong ngày, ngày trong tuần, [chỉ định: danh sách các thuộc tính bổ sung]]].

10.2 Các yêu cầu đảm bảo an toàn

Tất cả các yêu cầu đảm bảo an toàn được bao gồm trong Cấp bảo đảm đánh giá (EAL) 2 được bổ sung với các bổ sung sau đây:

- ALC_FLR.2: Khắc phục điểm yếu.

Dưới đây là danh sách các yêu cầu đảm bảo cần thiết cho hồ sơ bảo vệ này:

Bảng 9 - Các yêu cầu đảm bảo

Lớp đảm bảo	Các thành phần đảm bảo	Mô tả các thành phần đảm bảo
Phát triển	ADV_ARC.1	Mô tả kiến trúc an toàn.
	ADV_FSP.2	Đặc tả chức năng thực thi an toàn.
	ADV_TDS.1	Thiết kế cơ bản.
Tài liệu hướng dẫn	AGD_OPE.1	Hướng dẫn vận hành
	AGD_PRE.1	Các thủ tục chuẩn bị.
Hỗ trợ vòng đời	ALC_CMC.2	Sử dụng một hệ thống CM.
	ALC_CMS.2	Các thành phần của phạm vi CM TOE.
	ALC_DEL.1	Thủ tục giao nhận.
	ALC_FLR.2	Thủ tục báo cáo lỗi.
Kiểm thử	ATE_COV.1	Bằng chứng bảo đảm
	ATE_FUN.1	Kiểm thử chức năng.
	ATE_IND.2	Kiểm thử độc lập – mẫu.
Đánh giá lỗ hổng	AVA_VAN.2	Phân tích lỗ hổng.
Đánh giá đích an toàn	ASE_CCL.1	Tuyên bố phù hợp.
	ASE_ECD.1	Định nghĩa các thành phần mở rộng.
	ASE_INT.1	Giới thiệu ST.
	ASE_OBJ.2	Mục tiêu an toàn.
	ASE_REQ.2	Các yêu cầu an toàn dẫn xuất.
	ASE_SPD.1	Định nghĩa vấn đề an toàn.
	ASE_TSS.1	Đặc tả tóm tắt TOE.

11 Sở cứ

Phần này cung cấp sở cứ để lựa chọn các yêu cầu, mục tiêu, giả định, và các mối đe dọa về an toàn CNTT. Đặc biệt, nó cho thấy rằng các yêu cầu về an toàn CNTT phù hợp để đáp ứng các mục tiêu an toàn, do đó được thể hiện là phù hợp để bao gồm tất cả các khía cạnh của môi trường an toàn TOE.

11.1 Sở cứ các mục tiêu an toàn TOE

Các bảng sau đây cung cấp một ánh xạ của các mục tiêu an toàn cho môi trường được xác định bởi các mối đe dọa, chính sách và giả định, minh họa rằng mỗi mục tiêu an toàn bao gồm ít nhất một mối đe dọa, giả định hoặc chính sách và mỗi mối đe dọa, giả định hoặc chính sách đều được bao gồm bởi ít nhất một mục tiêu an toàn.

11.1.1 Phạm vi mục tiêu an toàn TOE

Bảng dưới đây tóm tắt các chính sách và các mối đe dọa liên quan đến các TOE.

Bảng 10 - Phạm vi mục tiêu an toàn TOE

Tên mục tiêu	Phạm vi SPD
O.ADMIN_ROLE	P.ACCOUNTABILITY P.ROLES T.ACCESS_TSFFUNC
O.AUDIT_GENERATION	P.ACCOUNTABILITY T.TSF_COMPROMISE
O.DISCRETIONARY_ACCESS	T.IA_USER T.UNAUTHORIZED_ACCESS
O.I&A	P.ACCOUNTABILITY T.ACCESS_TSFFUNC T.ACCESS_TSFDATA T.IA_MASQUERADE T.IA_USER
O.MANAGE	P.USER T.ACCESS_TSFDATA T.ACCESS_TSFFUNC T.UNAUTHORIZED_ACCESS
O.MEDIATE	T.IA_MASQUERADE T.UNAUTHORIZED_ACCESS T.IA_USER
O.RESIDUAL_INFORMATION	T.ACCESS_TSFDATA T.ACCESS_TSFFUNC T.RESIDUAL_DATA
O.TOE_ACCESS	P.ACCOUNTABILITY P.ROLES P.USER T.ACCESS_TSFDATA T.ACCESS_TSFFUNC T.IA_USER T.IA_MASQUERADE T.TSF_COMPROMISE

11.1.2 Sở cứ các mục tiêu an toàn TOE

Bảng sau mô tả sở cứ các mục tiêu an toàn của TOE:

Bảng 11 - Sở cứ các mục tiêu an toàn TOE

Mối đe dọa/ Chính sách	Mục tiêu an toàn TOE đề đáp ứng mối đe dọa/ chính sách	Cơ sở [illegible]
P.ACOUNTAVILITY Người dùng được ủy quyền của TOE sẽ phải chịu trách nhiệm cho hành động của họ trong TOE.	O.ADMIN_ROLE TOE sẽ cung cấp một cơ chế (ví dụ: một "vai trò") mà theo đó các hành động sử dụng đặc quyền quản trị có thể bị hạn chế.	O.ADMIN_ROLE hỗ trợ chính sách này bằng việc bảo đảm TOE có một mục tiêu để cung cấp các quản trị viên có thẩm quyền các quyền cần thiết để quản trị an toàn.
	O.AUDIT_GENERATION TOE phải cung cấp khả năng để phát hiện và tạo bản ghi sự kiện an toàn liên quan đến người dùng.	O.AUDIT_GENERATION hỗ trợ chính sách này bằng cách bảo đảm các bản ghi kiểm toán được tạo ra, cho khả năng được giải trình.
	O.I&A TOE phải đảm bảo rằng người dùng đã được xác thực trước khi TOE xử lý bất kỳ hành động nào cần xác thực.	O.I&A hỗ trợ chính sách này bằng cách yêu cầu mỗi thực thể tương tác với TOE phải được định danh và xác thực trước khi cho phép thực hiện bất kỳ hành động nào TOE đã định nghĩa chỉ cho người dùng đã xác thực.
	O.TOE_ACCESS TOE sẽ cung cấp các cơ chế kiểm soát truy cập logic của người dùng vào dữ liệu người dùng và TSF.	O.TOE_ACCESS hỗ trợ chính sách này bằng việc cung cấp cơ chế kiểm soát truy cập người dùng đã xác thực.

P.USER Quyền chỉ được trao cho những người dùng đáng tin cậy để thực hiện các hành động đúng đắn.	O.MANAGE TSF phải cung cấp tất cả các chức năng và phương tiện cần thiết để hỗ trợ người dùng được ủy quyền chịu trách nhiệm quản lý các cơ chế an toàn TOE, phải cho phép hạn chế các hành động quản lý như vậy đối với những người dùng riêng biệt và phải đảm bảo rằng chỉ có những người dùng được ủy quyền đó mới có thể truy cập các chức năng quản lý.	O.MANAGE hỗ trợ chính sách này bằng việc bảo đảm có các tiện ích và chức năng hỗ trợ vai trò quản trị viên có thẩm quyền.
	O.TOE_ACCESS TOE sẽ cung cấp các chức năng kiểm soát truy cập logic của người dùng vào dữ liệu người dùng và TSF.	O.TOE_ACCESS hỗ trợ chính sách này bằng việc cung cấp cơ chế kiểm soát truy cập người dùng đã xác thực.
	OE. ADMIN Những người chịu trách nhiệm về TOE là những cá nhân có thẩm quyền và đáng tin cậy, có khả năng quản lý TOE và an toàn thông tin trong nó.	OE. ADMIN hỗ trợ chính sách này bằng việc bảo đảm vai trò quản trị viên được hiểu rõ và sử dụng bởi các quản trị viên có thẩm quyền.

P.ROLES Quyền quản trị đối với chức năng TSF sẽ được trao cho nhân viên đáng tin cậy và bị hạn chế nhất có thể chỉ hỗ trợ nhiệm vụ quản trị của người có thẩm quyền. Vai trò này phải được tách bạch và phân biệt với những người dùng được ủy quyền khác.	O.ADMIN_ROLE TOE sẽ cung cấp một cơ chế (ví dụ: một "vai trò") mà theo đó các hành động sử dụng các đặc quyền quản trị có thể bị hạn chế.	O.ADMIN_ROLE TOE phải có mục tiêu để cung cấp một vai trò quản trị viên có thẩm quyền để quản trị an toàn. TOE có thể cung cấp các vai trò khác, nhưng vai trò của quản trị viên có thẩm quyền là phải có.
	O.TOE_ACCESS TOE sẽ cung cấp các chức năng kiểm soát truy cập logic của người dùng vào dữ liệu người dùng và TSF.	O.TOE_ACCESS hỗ trợ chính sách này bằng việc bảo đảm rằng vai trò quản trị viên có thể phân biệt với người dùng được ủy quyền khác.

T.ACCESS_TSFDATA Một tác nhân đe dọa có thể đọc hoặc sửa đổi dữ liệu TSF bằng cách sử dụng các chức năng của TOE mà không có sự cho phép thích hợp.	O.I&A TOE phải đảm bảo rằng người dùng đã được xác thực trước khi TOE xử lý bất kỳ hành động nào cần xác thực.	O.I&A hỗ trợ chính sách này bằng cách yêu cầu mỗi thực thể tương tác với TOE phải được định danh và xác thực trước khi cho phép thực hiện bất kỳ hành động nào TOE đã định nghĩa chỉ cho người dùng đã xác thực.
	O.MANAGE TSF phải cung cấp tất cả các chức năng và phương tiện cần thiết để hỗ trợ người dùng được ủy quyền chịu trách nhiệm quản lý các cơ chế an toàn TOE, phải cho phép hạn chế các hành động quản lý như vậy đối với những người dùng riêng biệt và phải đảm bảo rằng chỉ có những người dùng được ủy quyền đó mới có thể truy cập các chức năng quản lý.	O.MANAGE hỗ trợ chính sách này bằng việc bảo đảm có các tiện ích và chức năng hỗ trợ vai trò quản trị viên có thẩm quyền.
	O.RESIDUAL_INFORMATION TOE sẽ đảm bảo rằng bất kỳ thông tin nào chứa trong một tài nguyên được bảo vệ trong phạm vi kiểm soát của nó sẽ được chia sẻ lại chính xác khi phân bổ lại các tài nguyên này.	O.RESIDUAL_INFORMATION làm giảm mối đe dọa này vì thông tin sẽ được bảo vệ khỏi các tác nhân đe dọa thông qua các cuộc tấn công tái phân bổ (reallocation attack).
	O.TOE_ACCESS TOE sẽ cung cấp các chức năng kiểm soát truy cập logic của người dùng vào dữ liệu người dùng và TSF.	O.TOE_ACCESS Hỗ trợ chính sách này bằng một vai trò quản trị viên có thẩm quyền có thể phân biệt với người dùng được ủy quyền.

T.ACCESS_TSFFUNC Một tác nhân đe dọa có thể sử dụng hoặc quản lý TSF, bỏ qua các cơ chế bảo vệ của TSF.	O.ADMIN_ROLE TOE sẽ cung cấp một cơ chế (ví dụ: một "vai trò") mà theo đó các hành động sử dụng đặc quyền quản trị có thể bị hạn chế.	O.ADMIN_ROLE làm giảm mối đe dọa này bằng việc cô lập các hành động được phân quyền.
	O.I&A TOE phải đảm bảo rằng người dùng đã được xác thực trước khi TOE xử lý bất kỳ hành động nào cần xác thực.	O.I&A làm giảm mối đe dọa vì TOE yêu cầu xác thực thành công trước khi gán truy nhập tới bất kỳ nội dung kiểm soát truy cập nào. Bằng việc thực hiện xác thực mạnh để gán truy cập tới dịch vụ, một cơ hội của đối tượng tấn công giả danh một thực thể khác để truy cập trái phép tới dữ liệu hoặc tài nguyên TOE bị giảm.
	O.MANAGE TSF phải cung cấp tất cả các chức năng và phương tiện cần thiết để hỗ trợ người dùng được ủy quyền chịu trách nhiệm quản lý các cơ chế an toàn TOE, phải cho phép hạn chế các hành động quản lý như vậy đối với những người dùng riêng biệt và phải đảm bảo rằng chỉ có những người dùng được ủy quyền đó mới có thể truy cập các chức năng quản lý.	O.MANAGE làm giảm mối đe dọa vì chính sách kiểm soát truy cập được xác định để kiểm soát truy cập tới dữ liệu TSF. Mục tiêu này được sử dụng để chỉ ra ai có quyền xem và sửa đổi dữ liệu TSF, cũng như hoạt động của các chức năng TSF.
	O.RESIDUAL_INFORMATION TOE sẽ đảm bảo rằng bất kỳ thông tin nào chứa trong một tài nguyên được bảo vệ trong phạm vi kiểm soát của nó sẽ được chia sẻ lại chính xác khi phân bổ lại các tài nguyên này.	O.RESIDUAL_INFORMATION làm giảm mối đe dọa bằng việc bảo đảm dữ liệu TSF và dữ liệu người dùng không tiếp tục tồn tại khi một người dùng/tiến trình giải phóng tài nguyên này và cấp phát cho người dùng/tiến trình khác.
	O.TOE_ACCESS TOE sẽ cung cấp các chức năng kiểm soát truy cập logic của người dùng vào dữ liệu người dùng và TSF.	O.TOE_ACCESS làm giảm mối đe dọa vì làm cho tác nhân đe dọa không có khả năng truy cập tới TOE.

T.IA_MASSQUERADE Một người dùng hoặc một quá trình thay mặt người dùng có thể giả dạng thành một thực thể được ủy quyền để có quyền truy cập trái phép vào dữ liệu người dùng, dữ liệu TSF hoặc tài nguyên TOE	O.I&A TOE phải đảm bảo rằng người dùng đã được xác thực trước khi TOE xử lý bất kỳ hành động nào cần xác thực.	O.I&A làm giảm mối đe dọa bằng cách yêu cầu mỗi thực thể tương tác với TOP phải được định danh và xác thực thành công trước khi được phép thực hiện bất kỳ hành động nào TOE định nghĩa cho người dùng đã xác thực.
	O.MEDIATE TOE phải bảo vệ dữ liệu người dùng theo chính sách an toàn của nó và phải làm trung gian cho tất cả yêu cầu truy cập dữ liệu đó.	O.MEDIATE làm giảm mối đe dọa bằng cách bảo đảm tất cả truy cập tới dữ liệu người dùng phải được đưa tới thành phần trung gian, trừ khi dữ liệu được định danh là dữ liệu công khai. TOE yêu cầu xác thực thành công trước khi cấp quyền truy cập tới bất kỳ nội dung kiểm soát truy cập nào. Bằng cách thực hiện xác thực mạnh để gán quyền truy cập tới dịch vụ, cơ hội cho đối tượng tấn công giả mạo thực thể khác để truy cập trái phép vào dữ liệu và tài nguyên TOE sẽ giảm.
	O.TOE_ACCESS TOE sẽ cung cấp các chức năng kiểm soát truy cập logic của người dùng vào dữ liệu người dùng và TSF.	O.TOE_ACCESS làm giảm mối đe dọa bằng việc kiểm soát truy cập logic tới TOE và tài nguyên của TOE. Bằng việc hạn chế cách thức và thời điểm người dùng có thẩm quyền truy cập TOE và bằng cách ủy quyền loại và độ mạnh của cơ chế xác thực mục tiêu này giúp giảm khả năng người dùng cố gắng đăng nhập và giả mạo người dùng có thẩm quyền. Ngoài ra mục tiêu này cho phép quản trị viên kiểm soát số lần người dùng đăng nhập lỗi trước khi khóa tài khoản, hơn nữa giảm khả năng người dùng truy cập trái phép tới TOE.

T.IA_USER Một tác nhân đe dọa có thể có quyền truy cập vào dữ liệu người dùng, dữ liệu TSF hoặc tài nguyên TOE ngoại trừ các đối tượng công khai mà không được xác định và xác thực.	O.DISCRETIONARY_ACCESS TSF phải kiểm soát được truy cập của các đối tượng và/hoặc người dùng vào các tài nguyên được đặt tên dựa trên định danh chủ thể, đối tượng hoặc người sử dụng. TSF phải cho phép người dùng được ủy quyền được chỉ định cho mỗi chế độ truy cập mà người dùng/đối tượng được phép truy cập vào một đối tượng được đặt tên cụ thể trong chế độ truy cập đó.	O.DISCRETIONARY_ACCESS làm giảm mối đe dọa bằng việc yêu cầu dữ liệu bao gồm dữ liệu người dùng lưu trữ trong TOE có bảo vệ DAC.
	O.I&A TOE phải đảm bảo rằng người dùng đã được xác thực trước khi TOE xử lý bất kỳ hành động nào cần xác thực.	O.I&A làm giảm mối đe dọa bằng cách yêu cầu mỗi thực thể tương tác với TOE phải được định danh và xác thực trước khi được phép thực hiện bất kỳ hành động nào TOE định nghĩa cho người dùng đã xác thực.
	O.MEDIATE TOE phải bảo vệ dữ liệu người dùng theo chính sách an toàn của nó và phải làm trung gian cho tất cả yêu cầu truy cập dữ liệu đó.	O.MEDIATE làm giảm mối đe dọa bằng cách bảo đảm tất cả truy cập tới dữ liệu người dùng phải được đưa tới thành phần trung gian trừ khi dữ liệu được định danh là dữ liệu công khai. TOE yêu cầu xác thực thành công trước khi cấp quyền truy cập tới bất kỳ nội dung kiểm soát truy cập nào. Bằng cách thực hiện xác thực mạnh để gán quyền truy cập tới dịch vụ, thì giảm cơ hội cho đối tượng tấn công giả mạo thực thể khác để truy cập trái phép vào dữ liệu và tài nguyên TOE.
	O.TOE_ACCESS TOE sẽ cung cấp các chức năng kiểm soát truy cập logic của người dùng vào dữ liệu người dùng và TSF.	O.TOE_ACCESS làm giảm mối đe dọa bằng việc kiểm soát truy cập logic tới dữ liệu người dùng, dữ liệu TSF và tài nguyên của TOE.

T_RESIDUAL_DATA Một người dùng hoặc một quá trình thay mặt người dùng có thể có quyền truy cập trái phép vào dữ liệu người dùng hoặc TSF thông qua việc phân bổ lại tài nguyên TOE từ người dùng hoặc quá trình này sang người dùng hoặc quá trình khác.	O.RESIDUAL_INFORMATION TOE sẽ đảm bảo rằng bất kỳ thông tin nào chứa trong một tài nguyên được bảo vệ trong phạm vi kiểm soát của nó sẽ được chia sẻ lại chính xác khi phân bổ lại các tài nguyên này.	O.RESIDUAL_INFORMATION làm giảm mối đe dọa vì ngay cả khi cơ chế an toàn không cho phép người dùng xem dữ liệu TSF, nếu dữ liệu TSF tồn tại không phù hợp trong tài nguyên mà đưa ra cho người dùng thì người dùng này cũng không thể xem được dữ liệu TSF nếu không được ủy quyền.

T.TSF_COMPROMISE Một người dùng hoặc một quá trình thay mặt người dùng có thể khiến dữ liệu cấu hình bị truy cập không phù hợp (xem, sửa đổi hoặc xóa) hoặc có thể làm tổn hại mã thực thi trong TSF.	O.AUDIT_GENERATION TOE phải cung cấp khả năng để phát hiện và tạo bản ghi sự kiện an toàn liên quan đến người dùng.	O.AUDIT_GENERATION làm giảm mối đe dọa bằng việc cung cấp cho quản trị viên có thẩm quyền bản ghi kiểm toán phù hợp để hỗ trợ việc phát hiện TSF bị tấn công.
	O.TOE_ACCESS TOE sẽ cung cấp các chức năng kiểm soát truy cập logic của người dùng vào dữ liệu người dùng và TSF.	O.TOE_ACCESS làm giảm mối đe dọa do truy cập logic của người dùng tới TOE đã được kiểm soát sẽ làm giảm cơ hội của đối tượng tấn công truy cập tới dữ liệu cấu hình của TOE.

T_UNAUTHORIZED Một người dùng có thể có quyền truy cập trái phép vào dữ liệu người dùng mà họ không được phép theo chính sách an toàn TOE.	O.DISCRETIONARY_ACCESS TSF phải kiểm soát được việc truy cập của các đối tượng và/hoặc người dùng vào các tài nguyên được đặt tên dựa trên định danh chủ thể, đối tượng hoặc người sử dụng. TSF phải cho phép người dùng được ủy quyền được chỉ định cho mỗi chế độ truy cập mà người dùng/đối tượng được phép truy cập vào một đối tượng được đặt tên cụ thể trong chế độ truy cập đó.	O.DISCRETIONARY_ACCESS làm giảm mối đe dọa bằng việc yêu cầu dữ liệu bao gồm dữ liệu TSSF lưu trữ trong TOE có bảo vệ DAC.
	O.MANAGE TSF phải cung cấp tất cả các chức năng và phương tiện cần thiết để hỗ trợ người dùng được ủy quyền chịu trách nhiệm quản lý các cơ chế an toàn TOE, phải cho phép hạn chế các hành động quản lý như vậy đối với những người dùng riêng biệt và phải đảm bảo rằng chỉ có những người dùng được ủy quyền đó mới có thể truy cập các chức năng quản lý.	O.MANAGE làm giảm mối đe dọa bằng việc bảo đảm có các tiện ích và chức năng hỗ trợ quản trị viên có thể giải trình các hành động của họ với quản trị viên có ủy quyền.
	O.MEDIATE TOE phải bảo vệ dữ liệu người dùng theo chính sách an toàn của nó và phải làm trung gian cho tất cả yêu cầu truy cập dữ liệu đó.	O.MEDIATE làm giảm mối đe dọa bằng cách bảo đảm tất cả truy cập tới dữ liệu người dùng phải được đưa tới thành phần trung gian trừ khi dữ liệu được định danh là dữ liệu công khai. TOE yêu cầu xác thực thành không trước khi cấp quyền truy cập tới bất kỳ nội dung kiểm soát truy cập nào. Bằng cách thực hiện xác thực mạnh để gán quyền truy cập tới dịch vụ, thì giảm cơ hội cho đối tượng tấn công nghe lén và/hoặc dò đoán mật khẩu thành công. Cuối cùng TSSF phải đảm bảo tất cả chức năng bắt buộc đã cấu hình (xác thực, luật kiểm soát truy cập...) phải

		được thực hiện trước khi cho phép người dùng truy cập tới TOE và dịch vụ TOE. TOE giới hạn khả năng sửa đổi thuộc tính an toàn kết hợp với luật kiểm soát truy cập, truy cập tới dịch vụ đã xác thực và chưa xác thực cho quản trị viên. Tính năng này bảo đảm không người dùng nào có thể thay đổi thông tin theo chính sách để vượt qua chính sách an toàn TOE đã định nghĩa.

11.2 Sở cứ các mục tiêu an toàn cho môi trường hoạt động

Bảng sau cung cấp tóm tắt về giả định, chính sách và rủi ro liên quan đến các mục tiêu an toàn cho môi trường hoạt động.

Bảng 12 - Phạm vi SPD dành cho các mục tiêu an toàn cho môi trường hoạt động TOE

Tên	Phạm vi SPD
OE. ADMIN	A.MANAGE P.ACCOUNTABILITY P.ROLES P.USER
OE.INFO_PROTECT	A.AUTHUSER A.CONNECT A.MANAGE A.PHYSICAL A.TRAINEDUSER P.ACCOUNTABILITY P.USER T.TSF_COMPROMISE T.UNAUTHORIZED_ACCESS
OE.IT_I&A	A.SUPPORT
OE.IT_REMOTE	A.AUTHUSER A.CONNECT A.PEER_FUNC_&_MGT T.TSF_COMPROMISE

OE.IT_TRUSTED_SYSTEM	A.AUTHUSER A.CONNECT A.PEER_FUNC_&_MGT T.TSF_COMPROMISE
OE.NO_GENERAL_PURPOSE	A.NO_GENERAL_PURPOSE T.IA_MASQUERADE T.TSF_COMPROMISE
OE. PHYSICAL	A.CONNECT A.PHYSICAL T.TSF_COMPROMISE

Bảng sau cung cấp sở cứ các mục tiêu an toàn cho môi trường hoạt động.

Bảng 13 - Sở cứ các mục tiêu an toàn cho môi trường hoạt động TOE

Giả định	Mục tiêu an toàn cho môi trường hoạt động để đáp ứng giả định	Sở cứ cho việc xác định mục tiêu an toàn cho môi trường hoạt động
A.AUTHUSER Người dùng được ủy quyền sở hữu quyền truy cập cần thiết để truy cập ít nhất một số thông tin do TOE quản lý.	OE.INFO_PROTECT Những người chịu trách nhiệm về TOE phải thiết lập và thực hiện các thủ tục để đảm bảo rằng thông tin được bảo vệ một cách thích hợp. Đặc biệt: - Tất cả các mạng và cáp ngoại vi phải được phê duyệt để các dữ liệu nhạy cảm nhất được truyền qua. Các liên kết vật lý này được giả định là được bảo vệ đầy đủ để chống lại các mối đe dọa đối với tính bí mật và tính toàn vẹn của dữ liệu bằng các kỹ thuật bảo vệ logic và vật lý thích hợp. - Việc bảo vệ DAC trên các tệp tin có liên quan đến an toàn (chẳng hạn như các dấu vết kiểm toán và cơ sở dữ liệu ủy quyền) phải luôn được thiết lập chính xác. Người dùng được phép truy cập vào các phần của dữ liệu được quản lý bởi TOE và được đào tạo để kiểm soát dữ liệu của chính họ.	OE.INFO_PROTECT hỗ trợ giả định này bằng việc bảo người dùng được xác thực để truy cập tới các phần dữ liệu TOE quản lý và được đào tạo để thực hiện kiểm soát dữ liệu của họ. Người dùng đã xác thực và đào tạo được cung cấp thủ tục liên quan để bảo vệ thông tin hỗ trợ giả định cùng vận hành.

	OE.IT_REMOTE Nếu TOE dựa vào các hệ thống công nghệ thông tin đáng tin cậy từ xa để hỗ trợ thực thi chính sách của mình, các hệ thống này phải cung cấp các chức năng và dữ liệu được sử dụng bởi TOE trong việc đưa ra quyết định chính sách, đòi hỏi bởi TOE được bảo vệ đầy đủ từ bất kỳ cuộc tấn công nào có thể gây ra các chức năng đó để cung cấp kết quả sai.	OE.IT_REMOTE hỗ trợ giả định này bằng việc bảo đảm hệ thống từ xa – một phần của môi trường IT cũng được bảo vệ. Giả định này cho phép tin tưởng môi trường là an toàn.
	OE.IT_TRUSTED_SYSTEM Các hệ thống công nghệ thông tin đáng tin cậy từ xa thực hiện các giao thức và cơ chế yêu cầu của TSF để hỗ trợ thực thi chính sách an toàn. Các hệ thống công nghệ thông tin đáng tin cậy từ xa này được quản lý theo các chính sách đã biết, được chấp nhận và đáng tin cậy dựa trên các quy tắc và chính sách tương tự áp dụng cho TOE và được bảo vệ về mặt vật lý và logic tương đương với TOE.	OE.IT_TRUSTED_SYSTEM hỗ trợ giả định này bằng việc bảo đảm cung cấp hệ thống trong môi trường IT của TOE góp phần tạo một môi trường an toàn.

A.CONNECT Tất cả các kết nối đến và từ các hệ thống CNTT đáng tin cậy từ xa và giữa các phần riêng biệt của TSF đều được bảo vệ về mặt vật lý hoặc logic trong môi trường TOE để đảm bảo tính toàn vẹn và an toàn của dữ liệu được truyền và để đảm bảo tính xác thực của các điểm cuối truyền thông.	OE.IT_REMOTE Nếu TOE dựa vào các hệ thống công nghệ thông tin đáng tin cậy từ xa để hỗ trợ thực thi chính sách của mình, các hệ thống này phải cung cấp các chức năng và dữ liệu được sử dụng bởi TOE trong việc đưa ra quyết định chính sách, đòi hỏi bởi TOE được bảo vệ đầy đủ từ bất kỳ cuộc tấn công nào có thể gây ra các chức năng đó để cung cấp kết quả sai.	OE.IT_REMOTE hỗ trợ giả định này bằng việc đưa ra yêu cầu môi trường kết nối giữa các hệ thống tin cậy hoặc giữa các thành phần phân tách vật lý của TOE được bảo vệ đầy đủ khỏi các cuộc tấn công có thể là nguyên nhân chức năng đưa ra kết quả lỗi.
	OE.INFO_PROTECT Những người chịu trách nhiệm về TOE phải thiết lập và thực hiện các thủ tục để đảm bảo rằng thông tin được bảo vệ một cách thích hợp. Đặc biệt: - Tất cả các mạng và cáp ngoại vi phải được phê duyệt để các dữ liệu nhạy cảm nhất được truyền qua. Các liên kết vật lý này được giả định là được bảo vệ đầy đủ để chống lại các mối đe dọa đối với tính bí mật và tính toàn vẹn của dữ liệu bằng các kỹ thuật bảo vệ logic và vật lý thích hợp. - Việc bảo vệ DAC trên các tệp tin có liên quan đến an toàn (chẳng hạn như các dấu vết kiểm toán và cơ sở dữ liệu ủy quyền) luôn được thiết lập chính xác. Người dùng được phép truy cập vào các phần của dữ liệu được quản lý bởi TOE và được đào tạo để kiểm soát dữ liệu của chính họ.	OE.INFO_PROTECT hỗ trợ giả định bằng việc yêu cầu tất cả mạng và việc cắm dây mạng bên ngoài phải được áp dụng để truyền dữ liệu nhạy cảm qua kết nối. Các kết nối vật lý giả định được bảo vệ để chống lại mối đe dọa tới tính bí mật và tính toàn vẹn của dữ liệu truyền đi sử dụng kỹ thuật bảo vệ vật lý và logic phù hợp.
	OE.IT_TRUSTED_SYSTEM Các hệ thống công nghệ thông tin đáng tin cậy từ xa thực hiện các giao thức và cơ chế yêu cầu của TSF để hỗ trợ thực thi chính sách an toàn.	OE.IT_TRUSTED_SYSTEM hỗ trợ giả định này bằng việc bảo đảm hệ thống IT tin cậy ở xa thực hiện giao thức vào cơ chế TSF yêu cầu để hỗ trợ thực thi chính sách an toàn.

	Các hệ thống công nghệ thông tin đáng tin cậy từ xa này được quản lý theo các chính sách đã biết, được chấp nhận và đáng tin cậy dựa trên các quy tắc và chính sách tương tự áp dụng cho TOE và được bảo vệ về mặt vật lý và logic tương đương với TOE.	
	OE.PHYSICAL Những người chịu trách nhiệm về TOE phải đảm bảo rằng những thành phần của TOE quan trọng đối với việc thực thi chính sách an toàn được bảo vệ khỏi các cuộc tấn công vật lý có thể ảnh hưởng đến các mục tiêu an toàn công nghệ thông tin. Việc bảo vệ phải tương xứng với giá trị của các tài sản công nghệ thông tin được bảo vệ bởi TOE.	OE.PHYSICAL hỗ trợ giả định này bằng việc bảo đảm cung cấp an toàn vật lý phù hợp trong miền.
A.SUPPORT Bất kỳ thông tin nào được cung cấp bởi một thực thể đáng tin cậy trong môi trường CNTT và được sử dụng để hỗ trợ việc cung cấp thời gian và ngày tháng, thông tin được sử dụng trong chụp kiểm toán, xác thực người dùng và ủy quyền được sử dụng bởi TOE là chính xác và cập nhật.	OE.IT_I&A Bất kỳ thông tin nào được cung cấp bởi một thực thể đáng tin cậy trong môi trường và được sử dụng để hỗ trợ xác thực và ủy quyền của người dùng được sử dụng bởi TOE là chính xác và cập nhật.	OE.IT_I&A hỗ trợ ngầm giả định này.

A.MANAGE Chức năng an toàn TOE được quản lý bởi một hoặc nhiều quản trị viên có năng lực. Nhân viên quản trị hệ thống không được bắt cẩn, cố ý cẩu thả hoặc thù địch và sẽ tuân theo và chấp nhận các chỉ dẫn được cung cấp trong tài liệu hướng dẫn.	OE.ADMIN Những người chịu trách nhiệm về TOE là những cá nhân có năng lực và đáng tin cậy, có khả năng quản lý TOE và an toàn thông tin mà nó chứa.	OE.ADMIN hỗ trợ giả định do các quản trị viên được ủy quyền được coi là có đủ năng lực giúp bảo đảm tất cả nhiệm vụ và trách nhiệm được thực hiện một cách hiệu quả.
	OE.INFO_PROTECT Những người chịu trách nhiệm về TOE phải thiết lập và thực hiện các thủ tục để đảm bảo rằng thông tin được bảo vệ một cách thích hợp. Đặc biệt: - Tất cả các mạng và cáp ngoại vi phải được phê duyệt để các dữ liệu nhạy cảm nhất được truyền qua. Các liên kết vật lý này được giả định là được bảo vệ đầy đủ để chống lại các mối đe dọa đối với tính bí mật và tính toàn vẹn của dữ liệu bằng các kỹ thuật bảo vệ logic và vật lý thích hợp. - Việc bảo vệ DAC trên các tệp tin có liên quan đến an toàn (chẳng hạn như các dấu vết kiểm toán và cơ sở dữ liệu ủy quyền) luôn được thiết lập chính xác. Người dùng được phép truy cập vào các phần của dữ liệu được quản lý bởi TOE và được đào tạo để kiểm soát dữ liệu của chính họ.	OE.INFO_PROTECT hỗ trợ giả định bằng việc bảo đảm thành phần bảo vệ thông tin của TOE, các hệ thống và các kết nối liên quan tạo thành nền tảng cho TOE là quan trọng để giải quyết các vấn đề an toàn mô tả trong tiêu chuẩn này. Việc quản lý hiệu quả sử dụng thủ tục đã định nghĩa phụ thuộc vào quản trị viên có thẩm quyền.

A.NO_GENERAL_PURPOSE Không có khả năng lưu trữ hoặc tính toán cho mục đích chung có sẵn trên các máy chủ DBMS, ngoài các dịch vụ cần thiết cho hoạt động, quản trị và hỗ trợ của DBMS.	OE.NO_GENERAL_PURPOSE Sẽ không có khả năng tính toán cho mục đích chung (ví dụ: trình biên dịch hoặc ứng dụng người dùng) có sẵn trên các máy chủ DMBS, ngoài các dịch vụ cần thiết cho hoạt động, quản trị và hỗ trợ của DBMS....	OE.NO_GENERAL_PURPOSE Máy chủ DBMS không được có bất kỳ tính năng tính toán và lưu trữ. Giả định này sẽ bảo vệ dữ liệu TSFF khỏi các tiến trình độc hại. Mục tiêu của môi trường liên kết chặt chẽ với giả định, khi hoàn thành nội dung này thì sẽ giải quyết được các giả định.
A.PEER_FUNC_&_MGT Tất cả các hệ thống CNTT tin cậy từ xa được TSF tin cậy cung cấp dữ liệu hoặc dịch vụ TSF cho TOE hoặc để hỗ trợ TSF trong việc thực thi các quyết định chính sách an toàn được giả định để thực hiện chính xác chức năng được sử dụng bởi TSF phù hợp với các giả định được xác định cho chức năng này và được quản lý và vận hành hợp lý theo các ràng buộc chính sách an toàn tương thích với các ràng buộc của TOE.	OE.IT_REMOTE Nếu TOE dựa vào các hệ thống công nghệ thông tin đáng tin cậy từ xa để hỗ trợ thực thi chính sách của mình, các hệ thống này phải cung cấp các chức năng và dữ liệu được sử dụng bởi TOE trong việc đưa ra quyết định chính sách, đòi hỏi bởi TOE được bảo vệ đầy đủ từ bất kỳ cuộc tấn công nào có thể gây ra các chức năng đó để cung cấp kết quả sai.	OE.IT_REMOTE Giả định các kết nối giữa hệ thống tin cậy hoặc các phần phân tách vật lý của TOE được giải quyết bằng mục tiêu cụ thể mà hệ thống này được bảo vệ đầy đủ khỏi bất kỳ tấn công nào có thể làm cho các chức năng này cung cấp kết quả lỗi.
	OE.IT_TRUSTED_SYSTEM Các hệ thống công nghệ thông tin đáng tin cậy từ xa thực hiện các giao thức và cơ chế yêu cầu của TSF để hỗ trợ thực thi chính sách an toàn. Các hệ thống công nghệ thông tin đáng tin cậy từ xa này được quản lý theo các chính sách đã biết, được chấp nhận và đáng tin cậy dựa trên các quy tắc và chính sách tương tự áp dụng cho TOE và được bảo vệ về mặt vật lý và logic tương đương với TOE.	OE.IT_TRUSTED_SYSTEM Giả định tất cả hệ thống IT tin cậy ở xa thực hiện đúng chức năng TSF sử dụng với giả định đã định nghĩa cho chức năng này được hỗ trợ bằng các biện pháp bảo vệ logic và vật lý và áp dụng của chính sách tin cậy tương ứng tới TOE.

A.PHYSICAL Giả định rằng môi trường CNTT cung cấp cho TOE an toàn vật lý phù hợp, tương xứng với giá trị của tài sản CNTT được bảo vệ bởi TOE.	OE.PHYSICAL Những người chịu trách nhiệm về TOE phải đảm bảo rằng những thành phần của TOE quan trọng đối với việc thực thi chính sách an toàn được bảo vệ khỏi các cuộc tấn công vật lý có thể ảnh hưởng đến các mục tiêu an toàn công nghệ thông tin. Việc bảo vệ phải tương xứng với giá trị của các tài sản công nghệ thông tin được bảo vệ bởi TOE.	OE.PHYSICAL TOE, dữ liệu TSF và dữ liệu người dùng giả định được bảo vệ khỏi tấn công vật lý (trộm cắp, sửa đổi, phá hủy hoặc nghe lén). Tấn công vật lý có thể bao gồm xâm nhập trái phép với môi trường TOE, nhưng không bao gồm hành vi phá hủy môi trường vật lý do cá nhân nào đó có thẩm quyền truy cập môi trường TOE thực hiện.
	OE.INFO_PROTECT Những người chịu trách nhiệm về TOE phải thiết lập và thực hiện các thủ tục để đảm bảo rằng thông tin được bảo vệ một cách thích hợp. Đặc biệt: - Tất cả các mạng và cáp ngoại vi phải được phê duyệt để các dữ liệu nhạy cảm nhất được truyền qua. Các liên kết vật lý này được giả định là được bảo vệ đầy đủ để chống lại các mối đe dọa đối với tính bí mật và tính toàn vẹn của dữ liệu bằng các kỹ thuật bảo vệ logic và vật lý thích hợp. - Việc bảo vệ DAC trên các tệp tin có liên quan đến an toàn (chẳng hạn như các dấu vết kiểm toán và cơ sở dữ liệu ủy quyền) luôn được thiết lập chính xác. Người dùng được phép truy cập vào các phần của dữ liệu được quản lý bởi TOE và được đào tạo để kiểm soát dữ liệu của chính họ.	OE.INFO_PROTECT hỗ trợ giả định bằng việc yêu cầu tất cả mạng và việc cắm dây mạng bên ngoài phải được áp dụng để truyền dữ liệu nhạy cảm qua kết nối. Các kết nối vật lý giả định được bảo vệ để chống lại mối đe dọa tới tính bí mật và tính toàn vẹn của dữ liệu truyền đi sử dụng kỹ thuật bảo vệ vật lý và logic phù hợp.

A.TRAINEDUSER Người dùng được đào tạo đầy đủ và đáng tin cậy để hoàn thành một số nhiệm vụ hoặc nhóm nhiệm vụ trong môi trường CNTT an toàn bằng cách thực hiện kiểm soát hoàn toàn dữ liệu người dùng của họ.	OE.INFO_PROTECT Những người chịu trách nhiệm về TOE phải thiết lập và thực hiện các thủ tục để đảm bảo rằng thông tin được bảo vệ một cách thích hợp. Đặc biệt: - Tất cả các mạng và cáp ngoại vi phải được phê duyệt để các dữ liệu nhạy cảm nhất được truyền qua. Các liên kết vật lý này được giả định là được bảo vệ đầy đủ để chống lại các mối đe dọa đối với tính bí mật và tính toàn vẹn của dữ liệu bằng các kỹ thuật bảo vệ logic và vật lý thích hợp. - Việc bảo vệ DAC trên các tệp tin có liên quan đến an toàn (chẳng hạn như các dấu vết kiểm toán và cơ sở dữ liệu ủy quyền) luôn được thiết lập chính xác. Người dùng được phép truy cập vào các phần của dữ liệu được quản lý bởi TOE và được đào tạo để kiểm soát dữ liệu của chính họ.	OE.INFO_PROTECT hỗ trợ giả định này bằng việc bảo đảm người dùng được xác thực để truy cập tới các phần dữ liệu TOE quản lý và được đào tạo để thực hiện kiểm soát dữ liệu của họ.

Chính sách	Mục tiêu an toàn của môi trường để đáp ứng chính sách	Cơ sở xác định mục tiêu an toàn của môi trường
Người dùng TOE có thẩm quyền có thể giải trình được các hành động của họ	OE.ADMIN Những người chịu trách nhiệm về TOE là những cá nhân có năng lực và đáng tin cậy, có khả năng quản lý TOE và an toàn thông tin mà nó chứa.	OE.ADMIN hỗ trợ chính sách các quản trị viên có thẩm quyền được coi là có đủ năng lực để giúp bảo đảm tất cả nhiệm vụ và trách nhiệm được thực hiện một cách hiệu quả.
	OE.INFO_PROTECT Những người chịu trách nhiệm về TOE phải thiết lập và thực hiện các thủ tục để đảm bảo rằng thông tin được bảo vệ một cách thích hợp. Đặc biệt: Tất cả các mạng và cáp ngoại vi phải được phê duyệt để các dữ liệu nhạy cảm nhất được truyền qua. Các liên kết vật lý này được giả định là được bảo vệ đầy đủ để chống lại các mối đe dọa đối với tính bí mật và tính toàn vẹn của dữ liệu bằng các kỹ thuật bảo vệ logic và vật lý thích hợp. Việc bảo vệ DAC trên các tệp tin có liên quan đến an toàn (chẳng hạn như các dấu vết kiểm toán và cơ sở dữ liệu ủy quyền) luôn được thiết lập chính xác. Người dùng được phép truy cập vào các phần của dữ liệu được quản lý bởi TOE và được đào tạo để kiểm soát dữ liệu của chính họ.	OE.INFO_PROTECT hỗ trợ chính sách này bằng việc bảo đảm người dùng có thẩm quyền được đào tạo và có thủ tục để hỗ trợ họ và DAC bảo vệ chức năng, và có thể cung cấp đủ thông tin để thông báo cho những người yêu cầu giải trình.

P.ROLES TOE sẽ cung cấp vai trò quản trị viên có thẩm quyền để quản trị TOE an toàn. Vai trò này phải riêng biệt và khác biệt với những người dùng được ủy quyền khác.	OE.ADMIN Những người chịu trách nhiệm về TOE là những cá nhân có năng lực và đáng tin cậy, có khả năng quản lý TOE và an toàn thông tin mà nó chứa.	OE.ADMIN hỗ trợ chính sách bảo đảm một vai trò quản trị viên có thẩm quyền quản trị an toàn cho TOE đã thiết lập.
P.USER Quyền chỉ được trao cho người dùng đáng tin cậy để thực hiện các hành động một cách chính xác.	OE.ADMIN Những người chịu trách nhiệm về TOE là những cá nhân có năng lực và đáng tin cậy, có khả năng quản lý TOE và an toàn thông tin mà nó chứa.	OE.ADMIN hỗ trợ chính sách bằng việc bảo đảm quản trị viên có thẩm quyền, có trách nhiệm cấp quyền phù hợp cho người dùng và tin cậy.
	OE.INFO_PROTECT Những người chịu trách nhiệm về TOE phải thiết lập và thực hiện các thủ tục để đảm bảo rằng thông tin được bảo vệ một cách thích hợp. Đặc biệt: - Tất cả các mạng và cáp ngoại vi phải được phê duyệt để các dữ liệu nhạy cảm nhất được truyền qua. Các liên kết vật lý này được giả định là được bảo vệ đầy đủ để chống lại các mối đe dọa đối với tính bí mật và tính toàn vẹn của dữ liệu bằng các kỹ thuật bảo vệ logic và vật lý thích hợp. - Việc bảo vệ DAC trên các tệp tin có liên quan đến an toàn (chẳng hạn như các dấu vết kiểm toán và cơ sở dữ liệu ủy quyền) luôn được thiết lập chính xác.	OE.INFO_PROTECT hỗ trợ chính sách này bằng việc bảo đảm người dùng có thẩm quyền truy cập tới các phần dữ liệu TOE quản lý và được đào tạo để quản lý dữ liệu của họ và DAC bảo vệ các tập tin an toàn liên quan (như các dấu vết kiểm toán và cơ sở dữ liệu ủy quyền) phải luôn được cài đặt đúng.

	Người dùng được phép truy cập vào các phần của dữ liệu được quản lý bởi TOE và được đào tạo để kiểm soát dữ liệu của chính họ.	

Mối đe dọa	Mục tiêu an toàn môi trường để đáp ứng mối đe dọa	Cơ sở xác định mục tiêu an toàn môi trường
T.IA_MASQUERADE Người dùng hoặc một quá trình hành động thay mặt người dùng có thể giả trang thành một tổ chức được ủy quyền để có quyền truy cập trái phép vào dữ liệu người dùng, dữ liệu TSF hoặc tài nguyên TOE	OE.NO_GENERAL_PURPOSE Sẽ không có khả năng tính toán cho mục đích chung (ví dụ: trình biên dịch hoặc ứng dụng người dùng) có sẵn trên các máy chủ DMBS, ngoài các dịch vụ cần thiết cho hoạt động, quản trị và hỗ trợ của DBMS.	OE.NO_GENERAL_PURPOSE Máy chủ DBMS không được có bất kỳ tính năng tính toán và lưu trữ. Làm giảm mối đe dọa giả mạo vì chỉ người dùng DBMS hoặc chức năng liên quan được định nghĩa trong môi trường TOE.
T.TSF.COMPROMISE Người dùng hoặc một quá trình thay mặt người dùng có thể khiến dữ liệu cấu hình bị truy cập không phù hợp (xem, sửa đổi hoặc xóa) hoặc có thể làm tổn hại mã thực thi trong TSF.	OE.INFO_PROTECT Những người chịu trách nhiệm về TOE phải thiết lập và thực hiện các thủ tục để đảm bảo rằng thông tin được bảo vệ một cách thích hợp. Đặc biệt: - Tất cả các mạng và cáp ngoại vi phải được phê duyệt để các dữ liệu nhạy cảm nhất được truyền qua. Các liên kết vật lý này được giả định là được bảo vệ đầy đủ để chống lại các mối đe dọa đối với tính bí mật và tính toàn vẹn của dữ liệu bằng các kỹ thuật bảo vệ logic và vật lý thích hợp.	OE.INFO_PROTECT Giảm thiểu rủi ro bằng việc bảo đảm tất cả mạng và việc cắm dây mạng bên ngoài phải được áp dụng để truyền dữ liệu nhạy cảm qua kết nối. Các kết nối vật lý giả định được bảo vệ để chống lại mối đe dọa tới tính bí mật và tính toàn vẹn của dữ liệu truyền đi sử dụng kỹ thuật bảo vệ vật lý và logic phù hợp.

	- Việc bảo vệ DAC trên các tệp tin có liên quan đến an toàn (chẳng hạn như các dấu vết kiểm toán và cơ sở dữ liệu ủy quyền) luôn được thiết lập chính xác. Người dùng được phép truy cập vào các phần của dữ liệu được quản lý bởi TOE và được đào tạo để kiểm soát dữ liệu của chính họ.	
	OE.IT_REMOTE Nếu TOE dựa vào các hệ thống công nghệ thông tin đáng tin cậy từ xa để hỗ trợ thực thi chính sách của mình, các hệ thống này phải cung cấp các chức năng và dữ liệu được sử dụng bởi TOE trong việc đưa ra quyết định chính sách, đòi hỏi bởi TOE được bảo vệ đầy đủ từ bất kỳ cuộc tấn công nào có thể gây ra các chức năng đó để cung cấp kết quả sai.	OE.IT_REMOTE làm giảm mối đe dọa bằng việc bảo đảm hệ thống IT tin cậy ở xa được bảo vệ đầy đủ.
	OE.IT_TRUSTED_SYSTEM Các hệ thống công nghệ thông tin đáng tin cậy từ xa thực hiện các giao thức và cơ chế yêu cầu của TSF để hỗ trợ thực thi chính sách an toàn. Các hệ thống công nghệ thông tin đáng tin cậy từ xa này được quản lý theo các chính sách đã biết, được chấp nhận và đáng tin cậy dựa trên các quy tắc và chính sách tương tự áp dụng cho TOE và được bảo vệ về mặt vật lý và logic tương đương với TOE.	OE.IT_TRUSTED_SYSTEM làm giảm mối đe dọa bằng việc bảo đảm hệ thống IT tin cậy ở xa được quản lý theo chính sách tin cậy đã biết dựa trên quy tắc chung và chính sách TOE có thể chấp nhận và bảo vệ logic, vật lý tương ứng với TOE.
	OE.NO_GENERAL_PURPOSE Sẽ không có khả năng tính toán cho mục	OE.NO_GENERAL_PURPOSE làm giảm mối đe dọa bằng cách giảm

	đích chung (ví dụ: trình biên dịch hoặc ứng dụng người dùng) có sẵn trên các máy chủ DMBS, ngoài các dịch vụ cần thiết cho hoạt động, quản trị và hỗ trợ của DBMS	cơ hội loại bỏ tính năng không liên quan TOE trong môi trường TOE.
	OE.PHYSICAL Những người chịu trách nhiệm về TOE phải đảm bảo rằng những thành phần của TOE quan trọng đối với việc thực thi chính sách an toàn được bảo vệ khỏi các cuộc tấn công vật lý có thể ảnh hưởng đến các mục tiêu an toàn công nghệ thông tin. Việc bảo vệ phải tương xứng với giá trị của các tài sản công nghệ thông tin được bảo vệ bởi TOE.	OE.PHYSICAL làm giảm mối đe dọa một TSF bị tấn công do việc khai thác điểm yếu hoặc lỗ hổng vật lý như là một véc-tơ trong một tấn công.

T.UNAUTHORIZED_ACCESS Người dùng có thể có quyền truy cập trái phép vào dữ liệu người dùng mà họ không được phép theo chính sách an toàn TOE.	OE.INFO_PROTECT Những người chịu trách nhiệm về TOE phải thiết lập và thực hiện các thủ tục để đảm bảo rằng thông tin được bảo vệ một cách thích hợp. Đặc biệt: - Tất cả các mạng và cáp ngoại vi phải được phê duyệt để các dữ liệu nhạy cảm nhất được truyền qua. Các liên kết vật lý này được giả định là được bảo vệ đầy đủ để chống lại các mối đe dọa đối với tính bí mật và tính toàn vẹn của dữ liệu bằng các kỹ thuật bảo vệ logic và vật lý thích hợp. - Việc bảo vệ DAC trên các tệp tin có liên quan đến an toàn (chẳng hạn như các dấu vết kiểm toán và cơ sở dữ liệu ủy quyền) luôn được thiết lập chính xác. Người dùng được phép truy cập vào các phần của dữ liệu được quản lý bởi TOE và được đào tạo để kiểm soát dữ liệu của chính họ.	OE.INFO_PROTECT làm giảm rủi ro bằng việc bảo đảm các mối đe dọa vật lý và logic từ tất cả mạng và việc cắm dây mạng bên ngoài được bảo vệ phù hợp. Nếu thực hiện đúng cơ chế bảo vệ DAC thì có thể hỗ trợ việc xác định truy cập trái phép.

11.3 Sở cứ các yêu cầu chức năng an toàn

11.3.1 Sở cứ các yêu cầu chức năng an toàn mở rộng

Bảng sau đưa ra sở cứ cho yêu cầu chức năng an toàn mở rộng trong tiêu chuẩn này. Chú ý không có yêu cầu đảm bảo an toàn (SAR) mở rộng.

Bảng 14 - Sở cứ các yêu cầu chức năng an toàn mở rộng

Yêu cầu mở rộng	Định danh	Sở cứ
FIA_USB_(EXT).2	Nâng cao việc liên kết người dùng-đối tượng	Một DBMS có thể lấy được thuộc tính an toàn đối tượng từ dữ liệu TSF khác mà không phải trực tiếp từ thuộc tính an toàn người dùng. Một chính sách kiểm soát truy cập có thể sử dụng thuộc tính an toàn đối tượng này bên trong chính sách kiểm soát truy cập của nó, cho phép truy cập tới đối tượng quan trọng chỉ khi

		người dùng có kết nối thông qua cổng dữ liệu cụ thể.

11.3.2 Sở cứ các yêu cầu chức năng an toàn TOE

Bảng sau cung cấp sở cứ lựa chọn các yêu cầu chức năng an toàn. Dựa trên mỗi mục tiêu an toàn TOE để xác định yêu cầu chức năng toàn.

Bảng 15 - Sở cứ các yêu cầu chức năng an toàn mở rộng

Mục tiêu	Các yêu cầu để đáp ứng mục tiêu	Sở cứ
O.ADMIN_ROLE TOE sẽ cung cấp một cơ chế (ví dụ: một "vai trò") mà theo đó các hành động sử dụng đặc quyền quản trị có thể bị hạn chế.	FMT_SMR.1	TOE phải thiết lập ít nhất một vai trò quản trị có thẩm quyền. Tác giả ST có thể chọn xác định nhiều vai trò. Quản trị viên có thẩm quyền phải đưa ra quyền để thực hiện nhiệm vụ mà người dùng khác không thể thực hiện. Quyền bao gồm nhưng không giới hạn, truy cập tới thông tin kiểm toán và các chức năng an toàn (FMT_SMR.1).
O.AUDIT_GENERATION TOE phải cung cấp khả năng phát hiện và tạo bản ghi các sự kiện an toàn liên quan đến người dùng.	FAU_GEN.1 FAU_GEN.2 FAU_SEL.1	FAU_GEN.1 định nghĩa tập sự kiện TOE phải ghi lại. Yêu cầu này bảo đảm quản trị viên có khả năng kiểm toán tất cả sự kiện an toàn liên quan trong TOE. Yêu cầu này cũng định nghĩa thông tin phải có trong bản ghi kiểm toán với mỗi sự kiện có thể kiểm toán. Yêu cầu này cũng đưa ra mức độ chi tiết của bản ghi kiểm toán để ghi lại bất kỳ thông tin của yêu cầu chức năng an toàn bổ sung tác giả thêm vào tiêu chuẩn này. FAU_GEN.2 bảo đảm các bản ghi kiểm toán liên kết đến định danh một người dùng hoặc một nhóm với sự kiện có thể kiểm toán. Trong trường hợp người dùng đã xác thực, việc liên kết được thiết lập với ID của người dùng. Trong trường hợp nhóm đã xác thực thì liên kết được thiết lập với ID nhóm.

		FAU_SEL.1 cho phép quản trị viên định cấu hình các sự kiện có thể kiểm toán được ghi lại trong dấu vết kiểm toán. Điều này cung cấp cho quản trị viên tính linh hoạt trong việc ghi lại chỉ những sự kiện được coi là cần thiết theo chính sách của site, do đó làm giảm lượng tài nguyên tiêu thụ bởi cơ chế kiểm toán.
O.DISCRETIONARY_ACCESS TSF phải kiểm soát việc truy cập các đối tượng và/hoặc người dùng vào các tài nguyên được đặt tên dựa trên định danh của đối tượng, chủ thể hoặc người dùng. TSF phải cho phép người dùng được chỉ định cho mỗi chế độ truy cập mà người dùng/đối tượng được phép truy cập vào một đối tượng được đặt tên cụ thể trong chế độ truy cập đó.	FDP_ACC.1 FDP_ACF.1	TSF phải kiểm soát quyền truy cập vào các tài nguyên dựa trên định danh của người dùng được phép xác định tài nguyên nào họ muốn truy cập để lưu trữ dữ liệu của họ. Chính sách kiểm soát truy cập phải có một phạm vi kiểm soát được xác định [FDP_ACC.1]. Các quy tắc cho chính sách kiểm soát truy cập được xác định [FDP_ACF.1].
O.I&A TOE đảm bảo rằng người dùng được xác thực trước khi TOE xử lý bất kỳ hành động nào cần xác thực.	FIA_ATD.1 FIA_UAU.1 FIA_UID.1 FIA_USB_(EXT).2	TSF phải đảm bảo rằng chỉ những người dùng được ủy quyền mới có quyền truy cập vào TOE và các tài nguyên của nó. Người dùng được ủy quyền để truy cập TOE phải sử dụng quy trình định danh và xác thực [FIA_UID.1, FIA_UAU.1]. Để đảm bảo rằng các thuộc tính an toàn được sử dụng để xác định quyền truy cập được xác định và có sẵn cho các quyết định xác thực hỗ trợ. [FIA_ATD.1]. Sự ủy quyền phù hợp cho các chủ thể hoạt động thay mặt cho người sử dụng cũng được bảo đảm [FIA_USB_ (EXT).2].

		Đảm bảo độ bền thích hợp của cơ chế xác thực.
O.MANAGE TSF phải cung cấp tất cả các chức năng và phương tiện cần thiết để hỗ trợ người dùng có thẩm quyền chịu trách nhiệm quản lý các cơ chế an toàn TOE, phải cho phép hạn chế các hành động quản lý như vậy đối với người dùng chuyên dụng và phải đảm bảo rằng chỉ có những người dùng được ủy quyền đó mới có thể truy cập các chức năng quản lý.	FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_REV.1(1) FMT_REV.1(2) FMT_SMF.1 FMT_SMR.1	FMT_MOF.1 đòi hỏi khả năng sử dụng các tính năng TOE cụ thể được giới hạn cho quản trị viên. FMT_MSA.1 yêu cầu khả năng thực hiện các hoạt động đối với các thuộc tính an toàn được giới hạn trong các vai trò cụ thể. FMT_MSA.3 yêu cầu các giá trị mặc định được sử dụng cho các thuộc tính an toàn là hạn chế. FMT_MTD.1 yêu cầu khả năng thao tác nội dung TOE được giới hạn cho quản trị viên. FMT_REV.1 hạn chế khả năng thu hồi các thuộc tính cho quản trị viên. FMT_SMF.1 xác định các chức năng quản lý có sẵn cho quản trị viên có thẩm quyền. FMT_SMR.1 định nghĩa các vai trò an toàn cụ thể được hỗ trợ.
O.MEDIATE TOE phải bảo vệ dữ liệu người dùng theo chính sách an toàn của nó và phải làm trung gian cho tất cả yêu cầu truy cập dữ liệu đó.	FDP_ACC.1 FDP_ACF.1 FPT_TRC.1	Các yêu cầu FDP được lựa chọn để xác định chính sách, đối tượng và các hoạt động cho cách thức và khi nào sự điều đình diễn ra trong TOE. FDP_ACC.1 định nghĩa chính sách kiểm soát truy cập sẽ được thi hành trong danh sách các chủ thể hoạt động thay mặt cho người dùng cố gắng truy cập vào danh sách các đối tượng được đặt tên. Tất cả các hoạt động giữa chủ thể và đối tượng đó được xác định bởi chính sách của TOE. FDP_ACF.1 định nghĩa các thuộc tính an toàn được sử dụng để cung cấp kiểm soát truy cập cho các đối tượng dựa trên chính sách kiểm soát truy cập của TOE.

		FPT_TRC.1 đảm bảo dữ liệu TSF được sao chép xác định các thuộc tính cho kiểm soát truy cập phải nhất quán trên các thành phần phân tán của TOE. Yêu cầu này là để duy trì tính nhất quán của dữ liệu TSF được sao chép.
O.RESIDUAL_INFORMATION TOE sẽ đảm bảo rằng bất kỳ thông tin nào chứa trong một tài nguyên được bảo vệ trong phạm vi kiểm soát của nó không được tiết lộ không đúng khi tái phân bổ tài nguyên.	FDP_RIP.1	FDP_RIP.1 được sử dụng để đảm bảo nội dung của tài nguyên không có sẵn đối với các đối tượng khác ngoài những người được cấp quyền truy cập vào dữ liệu một cách rõ ràng.
O.TOE_ACCESS TOE sẽ cung cấp các cơ chế kiểm soát truy cập logic của người dùng vào dữ liệu người dùng và TSF.	FDP_ACC.1 FDP_ACF.1 FIA_ATD.1 FTA_MCS.1 FTA_TSE.1	FDP_ACC.1 yêu cầu mỗi kiểm soát truy cập được xác định SFP được đặt đúng chỗ cho một tập con của các hoạt động có thể trên một tập con của các đối tượng trong TOE. FDP_ACF.1 cho phép TSF thực thi truy cập dựa trên các thuộc tính an toàn và các nhóm thuộc tính được đặt tên. Hơn nữa, TSF có thể có thẩm quyền rõ ràng hoặc cho phép truy cập vào một đối tượng dựa trên các thuộc tính an toàn. FIA_ATD.1 định nghĩa các thuộc tính an toàn cho người dùng cá nhân bao gồm định danh người dùng và bất kỳ thành viên nhóm liên quan, các vai trò liên quan đến an ninh và các thuộc tính an toàn định danh khác. FTA_MCS.1 đảm bảo rằng người dùng chỉ có thể có tối đa số lượng các phiên hoạt động xác định mở tại bất kỳ thời điểm nào.

		FTA_TSE.1 cho phép TOE hạn chế các truy cập tới TOE dựa trên các tiêu chí nhất định.

11.3.3 Sở cứ đáp ứng các yêu cầu chức năng an toàn phụ thuộc

Bảng 16 - Sở cứ đáp ứng các yêu cầu chức năng an toàn phụ thuộc

Yêu cầu	Phụ thuộc	Đáp ứng
FAU_GEN.1	FPT_STM.1	Yêu cầu này được đáp ứng bởi giả định về môi trường IT đã đưa ra trong A.SUPPORT.
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	đáp ứng bởi FAU_GEN.1 đáp ứng bởi FIA_UID.1.
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	đáp ứng bởi FAU_GEN.1 đáp ứng bởi FMT_MTD.1.
FDP_ACC.1	FDP_ACF.1	đáp ứng bởi FDP_ACF.1.
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	đáp ứng bởi FDP_ACC.1 đáp ứng bởi FMT_MSA.3.
FDP_RIP.1	Không	N/A
FIA_ATD.1	Không	N/A
FIA_UAU.1	FIA_UID.1	đáp ứng bởi FIA_UID.1.
FIA_UID.1	Không	N/A
FIA_USB_(EXT).2	FIA_ATD.1	đáp ứng bởi FIA_ATD.1.
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	đáp ứng bởi FMT_SMF.1 đáp ứng bởi FMT_SMR.1.
FMT_MSA.1	[FDP_ACC.1 hoặc FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	đáp ứng bởi FDP_ACC.1 đáp ứng bởi FMT_SMF.1. đáp ứng bởi FMT_SMR.1.
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	đáp ứng bởi FMT_MSA.1 đáp ứng bởi FMT_SMR.1.

FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	đáp ứng bởi FMT_SMF.1 đáp ứng bởi FMT_SMR.1.
MT_REV.1(1)	FMT_SMR.1	đáp ứng bởi FMT_SMR.1.

11.4 Sở cứ đáp ứng các yêu cầu bảo đảm an toàn

Hồ sơ bảo vệ này được phát triển để sử dụng bởi các nhà phát triển phần mềm an toàn DBMS thương mại. Gói bảo đảm EAL 2 đã được lựa chọn để đạt được mức độ đảm bảo tối đa được công nhận trên phạm vi quốc tế thông qua CCRA.

Xử lý điểm yếu là yêu cầu duy nhất không có trong bất kỳ cấp độ EAL nào bởi vì nó không làm tăng thêm sự đảm bảo cho hệ thống hiện tại, mà cho các bản phát hành tiếp theo. Do đó, quyết định tăng EAL2 với ALC_FLR.2 để chỉ dẫn các nhà cung cấp về các kỹ thuật khắc phục lỗi thích hợp.

Các yêu cầu đảm bảo an toàn được đưa ra dựa trên các lập luận sau:

- EAL2 là hoàn toàn tự đáp ứng được với các phụ thuộc đã đáp ứng gói EAL2.
- Các yêu cầu bảo đảm an toàn mở rộng của EAL2 là ALC_FLR2 không có bất kỳ phụ thuộc nào.

Thư mục tài liệu tham khảo

[1] Protection Profile for Database Management Systems (DBMS PP) Base Package, Version 2.12, (*Hồ sơ bảo vệ cho hệ quản trị cơ sở dữ liệu (DBMS PP) Gói cơ sở, Phiên bản 2.12).*