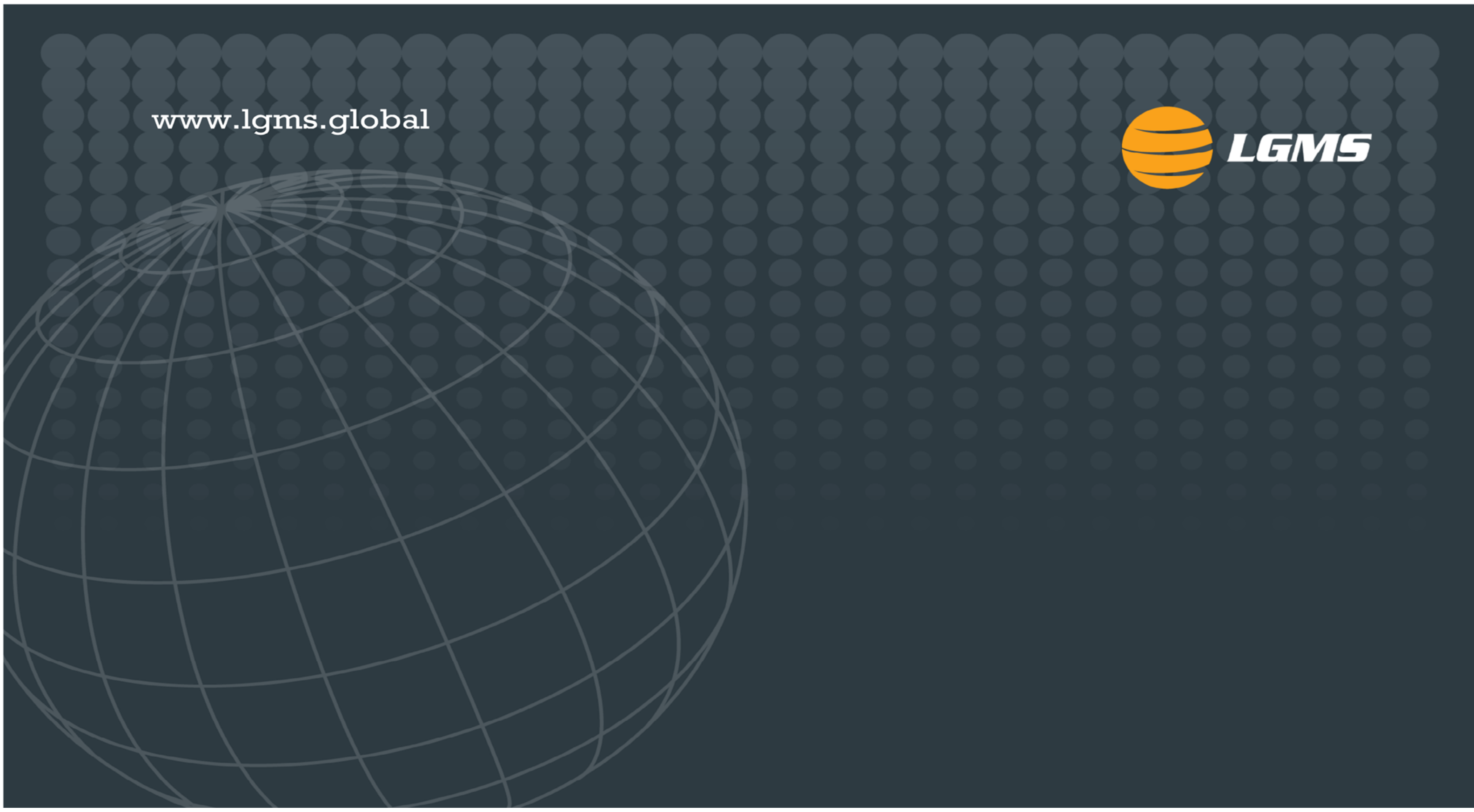

LGMS Security Assessment Report Generator Security Target

LE GLOBAL SERVICES SDN BHD

EAL 2

CONFIDENTIAL

[BLANK PAGE]

Document Details

Version	Date	Description	Author
2.0	10 December 2019	Security Target generated	KA Teoh

TABLE OF CONTENTS

1 SECURITY TARGET INTRODUCTION (ASE_INT)

This section identifies information as below:

- Security Target (ST) and Target of Evaluation (TOE) reference
- Document organization

1.1 SECURITY TARGET (ST) AND TARGET OF EVALUATION (TOE) REFERENCE

ST Title	LGMS Security Assessment Report Generator (LGMS Reporter) Security Target
ST Version	2.0, 10 December 2019
TOE Identification	LGMS Security Assessment Report Generator (LGMS Reporter), Version 1.0.0
Protection Profile (s)	N/A
Assurance Level	EAL 2
CC Identification	Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5 • Part 1: Introduction and General Model • Part 2: Security Functional Components • Part 3: Security Assurance Components Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 5 • Evaluation Methodology

1.2 DOCUMENT ORGANISATION

This document is divided into the following major sections:

1. Security Target (ST) Introduction
2. Target of Evaluation (TOE) Overview
3. Conformance Claim
4. Extended Components Definition
5. Security Problem Definition
6. Security Objectives
7. Security Functional Requirements (SFR)
8. Security Assurance Requirements (SAR)
9. Target of Evaluation (TOE) Summary Specification
10. Security Requirements Rationale

2 TOE OVERVIEW

The Target of Evaluation (TOE) is a web-based report generator which provides the service through Internet. TOE helps to simplify users experience as a one-stop presentation medium that displays the vulnerability assessment results in report.

2.1 TOE USAGE AND MAJOR SECURITY FEATURES

Users may upload raw files downloaded from vulnerability scanners to TOE, and generate a consolidated report. As different vulnerability scanners may have different naming convention for the same vulnerability, TOE is able to match against the same vulnerability across different vulnerability scanners, eliminate the repeated findings and only present the unique vulnerability in the generated report after consolidation. The TOE is able to support two (2) file types, for instance, ".xml" with specific data structure and ".nessus".

In addition, users are able to upload multiple raw files for different target servers, and consolidate all vulnerability results identified from multiple target servers into a single report. All raw files generated by vulnerability scanners are out of TOE scope.

The TOE provides browser-based clients with a unique ID assigned to each user. Upon successful authentication, users are able to perform the following activities in the TOE:

- Upload raw file generated by vulnerability scanner(s);
- Generate report with detailed analysis.

The TOE will then analyze and generate the report that includes the following information:

- Overall severity summary;
- Top 10 hosts with severity count;
- Severity statistic for all target servers;
- Severity summary of each severity level;
- Vulnerability details, which consists of:
  - Vulnerability description;
  - Recommended solution;
  - Evidence for reported vulnerability;
  - Reference URL (if applicable); and
  - CVSS score.

Fundamentally the TOE can be accessed by users through any web browser. The web application is hosted in a dedicated virtual machine managed by LE Global Services Sdn Bhd. The platform, virtual machine and SQL database are out of the TOE scope.

TOE provides the following security features, which are being claimed for this evaluation.

Security Features	Descriptions
Identification and Authentication	TOE identifies and authenticates users before the users are allowed to perform any actions within the TOE.
Security Audit Logs	TOE generates and store audit logs for the auditable events. Audit logs can only be viewed by the TOE administrators. The actions taken for audit logs review process are out of the TOE scope.

Trusted Path/Channels	TOE establishes secured and encrypted communication for data transfer *from* and *to* TOE.
User Data Protection	TOE manages access control policy to ensure user data are only accessible by authorized personnel.
Security Management	TOE supports the management of user's security attributes.

2.2 SUPPORTING NON-TOE HARDWARE

The following listed the hardware specifications where TOE is hosted. All specified hardwares are out of the TOE scope.

Hardware	Specification
CPU	2 cores x 2 threads
RAM	8 GB
Disk Space	100 GB

2.3 SUPPORTING NON-TOE SOFTWARE

The following listed the software and its version in the server which TOE is hosted. The softwares are out of the TOE scope.

Software	Version	Description
Operating System	Distributor ID: Ubuntu Description: Ubuntu 18.04.2 LTS Release: 18.04 Codename: bionic	Operating system used to host the application and related services.
Web Server	Apache Server 2.4	Web server used to run the web application.
Programming Language/ Framework	Language: PHP 7 Framework: Symfony 4	Programming language and framework used to develop the application.
Database Server	MySQL Server 5.7	Database system used for the application to store data.

2.4 CLIENT REQUIREMENTS

Any current web browser with JavaScript capability will be able to access the TOE. JavaScript must be enabled, and cookies must be enabled for browser-based sign-in and sign-out to work properly. Cookies that are used for authentication such as session cookie are always transfer through secure channel – Hyper Text Transfer Protocol Secure (HTTPS).

2.5 TOE DESCRIPTION

2.5.1 Physical scope of the TOE

TOE is a software application that provide the reporting services to users through Internet. The software application is installed in a dedicated virtual machine. The physical server that hosts the virtual machine is managed by LE Global Services Sdn Bhd. The platform, virtual machine and SQL database of the TOE are out of scope.

Users are able to access to TOE upon successful authentication through web browser and perform the operations. There is no installation required in order to access to the functions of the TOE. Physical scope is not applicable for this TOE.

2.5.2 Logical scope of the TOE

The logical boundaries and modules of the TOE are shown below:

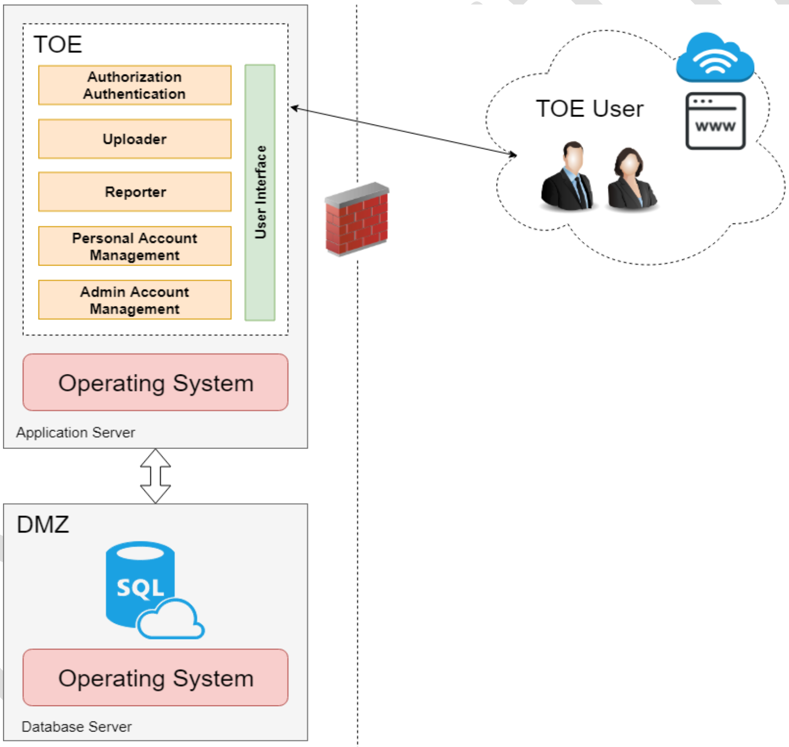

Figure 1 Logical Boundaries of the TOE

All hardware appliance, operating system, database system and application services used to support the TOE are not part of the scope of evaluation.

The TOE provides the feature for user to upload raw results from different vulnerability scanners, process the raw data and provide consolidated results. The TOE can only be used by the authenticated user via web browser. User will need to obtain the account username and password from administrator in order to use the TOE.

The TOE provides the following security features:

- **Identification and Authentication.**
  TOE will identify and authenticate the user before any actions can be performed. Unauthorized attempt will be recorded in the audit log.

- **Security Audit Logs.**
  TOE will generate audit logs for auditable events. These audit records can only be accessed by the TOE administrator.

- **Trusted Path/ Channels.**
  TOE provides the secure channel communication (HTTPS) between the TOE and TOE user.

- **User Data Protection.**
  TOE provides the feature to protect user data based on the role-based access control matrix and second layer authentication when generating the report.

- **Security Management.**
  TOE allows authenticated user to manage their own password. TOE administrator will be able to manage the user account such as update user's role and reset user's password.

3 CONFORMANCE CLAIM (ASE_CCL)

3.1 COMMON CRITERIA CONFORMANCE CLAIM

This ST and TOE are conformant to version 3.1 (Revision 5) of the Common Criteria for Information Technology Security Evaluation. Specific conformance claims are as below:

- **Part 2 conformant.**
  Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, version 3.1 (Rev 5).
- **Part 3 conformant.**
  Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, version 3.1 (Rev 5).

3.2 PROTECTION PROFILE CLAIM

This ST does not claim conformance to any Protection Profile.

3.3 PACKAGE CLAIM

The ST is conformant to EAL 2 assurance package as defined in Part 3 of Common Criteria version 3.1 (Rev 5).

3.4 CONFORMANCE CLAIM RATIONALE

No conformance claim rationale is necessary as this ST does not claim conformance to Protection Profile.

4 EXTENDED COMPONENTS DEFINITION (ASE_ECD)

This TOE does not consist of any extended components, hence the requirements for the Extended Components Definition (ASE_ECD) are not applicable.

5 SECURITY PROBLEM DEFINITION (ASE_SPD)

This section describes the nature of security problem that are intended to be addressed by TOE, which is described through:

- Known or assumed threats which TOE shall addressed;
- Organizational security policies that specify rules or guidelines for TOE users to comply with;
- Assumptions about the security aspects of the environment which TOE is intended to operate.

5.1 THREATS

The followings are the threats identified for TOE. TOE is responsible for addressing the threats to the environment where it resides.

Threat Identifier	Threat Statement
T.BROKEN_AUTH	An unauthorized individual may attempt to bypass the authentication function to access the TOE data.
T.BROKEN_ACCESS	An authorized user may attempt to bypass his/her assigned privilege to access unauthorized TOE data or restricted information.
T.MAL_UPLOAD	An authorized user may attempt to upload malicious files intentionally or unintentionally, causing TOE to be exploited via remote command execution.
T.MAL_INTERCEPTION	An unauthorized individual may sniff or intercept the communication between TOE and TOE user.

5.2 ORGANIZATIONAL SECURITY POLICIES

The followings are the Organizational Security Policies (OSP) expected to be imposed by an organization to secure the TOE and its environment.

OSP Identifier	OSP Statement
P.ROLE	Only authorized user that is approved by the TOE administrator is granted with access to the TOE, based on the role assigned.
P.PASSWORD	Authorized TOE users shall use strong password with the combination of uppercase character, lowercase character, digit, special character and minimum 8 characters.

5.3 ASSUMPTIONS

The following assumptions describes the security aspect of TOE and operational environment in which the TOE is deployed.

Assumption	Assumption Description
A.PHY	It is assumed that the TOE and its platform are located within secured facilities with controlled access to prevent unauthorized physical access.
A.TIMESTAMP	It is assumed that the TOE operational environment is able to provide reliable timestamp for TOE which will affect the time accuracy of audit logs.
A.ADMIN	It is assumed that authorized TOE administrators have no malicious intention; and are appropriately trained to undertake the configuration and management of the TOE.

6 SECURITY OBJECTIVES (ASE_OBJ)

This section provides the security objectives which address the threats, assumptions and Organizational Security Policies as per described in earlier chapter “Security Problem Definition”.

6.1 SECURITY OBJECTIVES FOR TOE

Security Objectives for TOE	Description
O.AUTHENTICATE	TOE shall implement security mechanisms to prevent unauthenticated access such as brute force attempts made by unauthorized individual. Threats: T.BROKEN_AUTH OSP: P.PASSWORD
O.SEC_ACCESS	TOE shall provide mechanisms that control user’s logical access to the TOE and explicitly deny access that is beyond the assigned privilege. Threats: T.BROKEN_ACCESS OSP: P.ROLE
O.MAL_UPLOAD	TOE shall perform validation on the files uploaded prior processing it. Threats: T.MAL_UPLOAD
O.SEC_PROTOCOL	TOE shall enforce data sent between TOE and TOE user via secured channel only. Threats: T.MAL_INTERCEPTION

6.2 SECURITY OBJECTIVES FOR OPERATIONAL ENVIRONMENT

Security Objectives for Operational Environment	Description
OE.PHY	The TOE must be installed and operated in a physically secure area.
OE.TRUSTED_TIMESTAMP	The TOE environment shall provide reliable timestamps to the TOE.
OE.TRUSTED_ADMIN	Administrators of TOE shall be non-hostile while managing the TOE, and shall receive proper training on TOE management.

7 SECURITY FUNCTIONAL REQUIREMENTS (ASE_REQ)

This section specifies Security Functional Requirements (SFRs) of the ST which consists of the following components from CC Part 2, summary as below:

Class Family	Description	Dependencies
Class FIA: Identification and Authentication		
FIA_AFL.1	Authentication failures handling	FIA_UAU.1 Timing of authentication
FIA_ATD.1	User attribute definition	No dependencies
FIA_SOS.1	Verification of secrets	No dependencies
FIA_UAU.1	Timing of authentication	FIA_UID.1 Timing of identification
FIA_UID.1	Timing of identification	No dependencies
Class FAU: Security Audit		
FAU_GEN.1	Security audit data generation	FPT_STM.1 Reliable time stamps
FAU_GEN.2	User identity association	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification
Class FTP: Trusted Path/Channels		
FTP_TRP.1	Trusted path	No dependencies
Class FDP: User Data Protection		
FDP_ACC.1	Subset access control	FDP_ACF.1 Security attribute role-based access control
FDP_ACF.1	Security attribute role-based access control	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
Class FMT: Security Management		
FMT_MSA.1	Management of security attributes	FDP_ACC.1 Subset access control FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions
FMT_MSA.3	Static attribute initialization	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_SMR.1	Security roles	FIA_UID.1 Timing of identification
FMT_SMF.1	Specification of management functions	No dependencies

7.1 CLASS FIA: IDENTIFICATION AND AUTHENTICATION

7.1.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1	The TSF shall detect when [**five (5)**] unsuccessful authentication attempts occur related to **user authentication during login**.
FIA_AFL.1 .2	When the defined number of unsuccessful authentication attempts has been [**surpassed**], the TSF shall [**lockout user account for a period of time, which is 30 minutes**].

Application Note:

1) This requirement stipulates the rules of authentication failure handling and use to prevent brutefoce attack.

7.1.2 FIA_ATD.1 User attribute definition

FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: a) [User identity: **Username**; b) Authentication: **Password**; c) Authorization: **Roles (privileges)**; d) User registration detail: **Email address**].

Application Note:

1) This requirement defines the security attributes to maintain for each individual user. These attributes will be used for security control purposes such as access control.

7.1.3 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet: a) [**at least 8 characters**; b) **at least 1 uppercase character (A-Z)**; c) **at least 1 lowercase character (a-z)**; d) **at least 1 digit (0-9)**; e) **at least 1 special character**].

Application Note:

1) This requirement stipulates the rules of password complexity, to strengthen the user password during the account creation and password reset process.

7.1.4 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1	The TSF shall allow [**entry of username and password**] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note:

1) This requirement defines the action and behavior of user authentication process.

7.1.5 FIA_UID.1 Timing of identification

FIA_UID.1.1	The TSF shall allow [**entry of username and password**] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note:

1) This requirement defines the action and behavior of user identification process.

7.2 CLASS FAU: SECURITY AUDIT

7.2.1 FAU_GEN.1 Security audit data generation

FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [**basic**] level of audit; and c) [**Attempts of** **i) uploading invalid file type/malicious files** **ii) user authentication process** **iii) change of security attributes**].
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**none**].

Application Note:

1) This requirement defines the events and details needed to be logged for auditing purposes.

7.2.2 FAU_GEN.2 User identity association

FAU_GEN.2.1	For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Application Note:

1) This requirement stipulates that each logged event shall be associate to the user that caused the event for auditing and tracking purposes.

7.3 CLASS FTP: TRUSTED PATH/CHANNELS

7.3.1 FTP_TRP.1 Trusted path

FTP_TRP.1.1	The TSF shall provide a communication path between itself and [**remote**] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [**modification, disclosure**].
FTP_TRP.1.2	The TSF shall permit [**remote users**] to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for [**communication between TOE User and TOE Application (HTTPS Protocol - TLS)**].

Application Note:

1) This requirement defines the encryption method used to protect communication data between TOE and TOE User.

7.4 CLASS FDP: USER DATA PROTECTION

7.4.1 FDP_ACC.1 Subset access control

FDP_ACC.1.1	The TSF shall enforce the [**Role-Based Access Control**] on [Subjects: a) **authenticated and authorised users**; Objects: a) **reporting data**; b) **user data**; Operations: a) **upload raw file**; b) **generate report**; c) **update personal password**; d) **access to admin panel**].

Application Note:

1) This requirement lists the subjects, objects and operations to be enforced based on the role-based access control matrix.

7.4.2 FDP_ACF.1 Security attribute role-based access control

FDP_ACF.1.1	The TSF shall enforce the [**Role-Based Access Control**] to objects based on the following: [Subjects: a) **authenticated and authorised users**; Objects: a) **reporting data**; b) **user data**; Security Attributes: a) **Username**;

	b) **Password**; c) **Role**; d) **Access Code**].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [a) **username, password and role are correct during uploading raw file**; b) **username, password, role and access code are correct during generating report**; c) **username, password and role are correct during updating personal profile**; d) **username, password and role are correct during accessing admin panel**].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].

Application Note:

1) This requirement lists the subjects, objects and security attributes to be enforced based on the role-based access control matrix.
2) This requirement also defines the behavior and rule for operations between controlled subjects and controlled objects.

7.5 CLASS FMT: SECURITY MANAGEMENT

7.5.1 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1	The TSF shall enforce the [**Role-Based Access Control**] to restrict the ability to [**query and modify**] the security attributes [**username, password, role and email address**] to [**users**].

Application Note:

1) This requirement lists the actions toward security attributes to be enforced based on the role-based access control matrix.

7.5.2 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1	The TSF shall enforce the [**Role-Based Access Control**] to provide [**permissive**] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [**administrator**] to specify alternative initial values to override the default values when an object or information is created.

Application Note:

1) This requirement defines the default behavior for the used of security attributes to enforce SFP. Only user with ADMINSTRATOR role is allowed to modified the security attributes.

7.5.3 FMT_SMR.1 Security roles

FMT_SMR.1.1	The TSF shall maintain the roles [**administrator, user, upload, generate**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

Application Note:

1) ADMINISTRATOR role allow user to access all modules of TOE.
2) USER role only allow user to access to Login, Dashboard, Upload, Generate Report and Personal Profile modules.
3) UPLOAD role only allow user to access to Login, Dashboard and Upload modules.
4) GENERATE role only allow user to access to Login, Dashboard and Generate Report modules.
5) The roles will be used by the TOE for access control purposes.

7.5.4 FMT_SMF.1 Specification of management functions

FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [a) **Create account**; b) **Activate/ inactivate;** c) **Assign user privilege**; d) **Reset password**; e) **Unlock/ lock account**].

Application Note:

1) This requirement defines the administrative management functions that can only access and perform by user who has ADMINISTRATOR role.

8 SECURITY ASSURANCE REQUIREMENTS (ASE_REQ)

This ST implements the Security Assurance Requirements (SARs) of the Evaluation Assurance Level 2 (EAL2) package. The assurance components are summarized in the following table which is drawn from CC Part 3:

Assurance Class	Assurance Components
Development	ADV_ARC.1
	ADV_FSP.2
	ADV_TDS.1
Guidance Documents	AGD_OPE.1
	AGD_PRE.1
Life-cycle Support	ALC_CMC.2
	ALC_CMS.2
	ALC_DEL.1
Security Target Evaluation	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
Tests	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
Vulnerability Assessment	AVA_VAN.2

9 TOE SUMMARY SPECIFICATION

This section specifies the security functional requirements addressed by the TOE.

9.1 IDENTIFICATION AND AUTHENTICATION

TOE provides user interfaces which allow administrator to manage the TOE security attributes. The user interface provides web-based access to TOE functions through web browsers. The user interface module enforced identification and authentication mechanism before any user can perform any actions on the TOE.

Users are required to set their password according to a defined password requirement, where the minimum characters are set to eight (8) characters, and fulfil at least three (3) from the followings:

i. at least 1 uppercase character (A-Z);
ii. at least 1 lowercase character (a-z);
iii. at least 1 digit (0-9);
iv. at least 1 special character.

The authentication attempts are monitored and controlled by the TOE, where the account will be lockout after five (5) invalid attempts.

TOE maintains the information that determines the access level of each user and administrator to TOE function modules.

The TOE maintains the following list of security attributes belonging to individual users:

i. Username (Unique identification code);
ii. Password;
iii. Roles (privileges);
iv. Email.

Security Functional Requirements Satisfied: FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UID.1

9.2 SECURITY AUDIT

Audit logs are generated by the TOE with the association of the user and the event. All the auditable events are logged with a user who performs the operation within the TOE.

The events will be logged by the TOE as below:

i. Uploading invalid file type/malicious files
ii. User authentication process
iii. Change of security attributes

Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2

9.3 TRUSTED PATH/CHANNEL

TOE provides the secured and encrypted communication channel between the data transfer *to* and *from* the TOE. Users will be always accessing the TOE through HTTPS web protocol which will use Transport Layer Security (TLS) for the encryption. The encryption protocols require minimum version of 1.2 and all SSL protocols will not be supported.

Security Functional Requirements Satisfied: FTP_TRP.1

9.4 USER DATA PROTECTION

The TOE access control list will be predefined for each role. All TOE functions will be automatically map to the access control list before the user is granted to perform any actions in the TOE.

Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1

9.5 SECURITY MANAGEMENT

Management interface allows administrator to manage the TOE security attributes. TOE will ensure the security management function is only allow to be accessed by the administrator only.

Administrator will be able to perform the administrative action as below:

i. Create account;
ii. Activate/ inactivate account;
iii. Assign user privilege;
iv. Reset password;
v. Unlock/ lock account.

The list of the roles is predefined in the TOE.

Security Functional Requirements Satisfied: FMT_MSA.1, FMT_MSA.3, FMT_SMR.1, FMT_SMF.1

10 SECURITY REQUIREMENTS RATIONALE

10.1 SECURITY OBJECTIVES RATIONALE

This section explains how security objectives are related to each other. The following table shows threat, organizational security policy and assumptions being mapped to security objectives.

THREATS/ **POLICIES/** **ASSUMPTIONS** **OBJECTIVES**	**T.BROKEN_AUTH**	**T.BROKEN_ACCESS**	**T.MAL_UPLOAD**	**T.MAL_INTERCEPTION**	**P.ROLE**	**P.PASSWORD**	**A.PHY**	**A.TIMESTAMP**	**A.ADMIN**
O.AUTHENTICATE	✓					✓			
O.SEC_ACCESS		✓			✓				
O.MAL_UPLOAD			✓						
O.SEC_PROTOCOL				✓					
OE.PHY							✓		
OE.TRUSTED_TIMESTAMP								✓	
OE.TRUSTED_ADMIN									✓

10.1.1 Rationale for Security Objectives Mapped to Threats

Threats	Security Objectives	Rationale
T.BROKEN_AUTH	O.AUTHENTICATE	This security objective ensures the user is properly authenticated before the user is allowed to access the TOE.
T.BROKEN_ACCESS	O.SEC_ACCESS	This security objective ensures the user is only allowed to access the assigned TOE function and explicitly deny access that is beyond the assigned privilege.
T.MAL_UPLOAD	O.MAL_UPLOAD	This security objective ensures the uploaded files are legitimate and with a proper file extension.
T.MAL_INTERCEPTION	O.SEC_PROTOCOL	This security objective ensures the TOE data is being protected and secured when transfer *from* or *to* the TOE.

10.1.2 Rationale for Security Objectives Mapped to OSP

OSP	Security Objectives	Rationale
P.ROLE	O.SEC_ACCESS	This security objective ensures the OSP is fulfilled by restricting user access based on the role assigned.

P.PASSWORD	O.AUTHENTICATE	This security objective ensures the OSP is fulfilled by implementing secure password policy.

10.1.3 Rationale for Security Objectives Mapped to Assumptions

Assumptions	Security Objectives	Rationale
A.PHY	OE.PHY	This security objective counters assumption because the TOE and its environment shall be physically secure.
A.TIMESTAMP	OE.TRUSTED_TIMESTAMP	This security objective counters assumption because TOE environment shall provide reliable time stamps.
A.ADMIN	OE.TRUSTED_ADMIN	This security objective counters assumption because the TOE administrator shall be non-hostile while managing the TOE, and will be properly trained on TOE management.

10.2 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

10.2.1 Rationale for SFR Mapped to Security Objectives

Security Objectives	SFR	Rationale
O.AUTHENTICATE	FIA_AFL.1	This SFR will identify unsuccessful authentication and locked the user account for 30 minutes if the continuous failure attempt is more than 5 times.
	FIA_SOS.1	This SFR will ensure user's password complexity is meet.
	FAU_GEN.1	This SFR will generate audit log on the event of successed and failed login attempts.
	FAU_GEN.2	This SFR will include the user's unique identifier (username) on the audit log.
O.SEC_ACCESS	FIA_ATD.1	This SFR will maintain list of security attributes belonging to individual user.
	FDP_ACC.1	This SFR will ensure the access to TOE operation is based on the assigned role.
	FDP_ACF.1	This SFR will ensure the access to TOE data is restricted to the owner of data or authorized users.
	FMT_MSA.1	This SFR will ensure only administrator is allowed to access the security attributes data.
	FMT_MSA.3	This SFR will ensure only permitted users are allow to access the TOE function based on the assigned role.

	FMT_SMR.1	This SFR defines the TOE’s user role and its relationship.
	FMT_SMF.1	This SFR defines the management functionality.
O.MAL_UPLOAD	FAU_GEN.1	This SFR will create audit log on invalid file type or malicious files upload.
	FAU_GEN.2	This SFR will include the user’s unique identifier (username) on the audit log.
O.SEC_PROTOCOL	FTP_TRP.1	This SFR provides secured and encrypted communication for data transfer *from* and *to* TOE.

10.2.2 SFR Dependency Rationale

Table below identifies the SFR from Part 2 CC and the associated dependencies. It indicates whether the ST explicitly addresses each dependency.

Class Family	Dependencies	Dependency Satisfied	Justification
FIA_AFL.1	FIA_UAU.1	Yes	-
FIA_ATD.1	-	-	-
FIA_SOS.1	-	-	-
FIA_UAU.1	FIA_UID.1	Yes	-
FIA_UID.1	-	-	-
FAU_GEN.1	FPT_STM.1	No	TOE environment shall provide reliable timestamps to the TOE
FAU_GEN.2	FAU_GEN.1	Yes	-
	FIA_UID.1	Yes	-
FTP_TRP.1	-	-	-
FDP_ACC.1	FDP_ACF.1	Yes	-
FDP_ACF.1	FDP_ACC.1	Yes	-
	FMT_MSA.3	Yes	-
FMT_MSA.1	FDP_ACC.1	Yes	-
	FMT_SMR.1	Yes	-
	FMT_SMF.1	Yes	-
FMT_MSA.3	FMT_MSA.1	Yes	-
	FMT_SMR.1	Yes	-
FMT_SMR.1	FIA_UID.1	Yes	-
FMT_SMF.1	-	-	-

[END OF DOCUMENT]