24 JAN 2026

Document Version 1.1

MEJA BULAT VERSION 5.15.3

SECURITY TARGET

INFOSYS GATEWAY

For more information visit us at
www.infosysgateway.com.my

Document management

Document identification

Document title	Meja Bulat Version 5.15.3 Security Target
Document version	1.1
Document date	24-JAN-2026
Release Authority	Infosys Gateway Sdn Bhd

Document history

Version	Date	Description
0.1	17-FEB-2025	Initial Released
0.2	19-MAY-2025	Update Section 1 until Section 6 based on comments from the lab and certification body
1.0	19-DEC-2025	Update document based on EAL1 requirement Final Released
1.1	24-JAN-2026	Update Section 2 until Section 4

Table of Contents

1 Security Target Introduction 5

1.1 ST Reference 5

1.2 TOE Reference 5

1.3 Document Organization 5

1.4 Defined Terms 6

1.5 TOE Overview 7

1.5.1 TOE Usage and Major Security Functions 7

1.5.2 TOE Type 8

1.5.3 Supporting Hardware, Software and/or Firmware 8

1.6 TOE Description 9

1.6.1 Physical Scope of the TOE 9

1.6.2 Logical Scope of the TOE 10

2 Conformance Claim 12

3 Security Problem Definition 13

3.1 Overview 13

3.2 Threats 13

3.3 Organisational security policies 13

3.4 Assumptions 13

4 Security objectives 15

4.1 Overview 15

4.2 Security objectives for the environment 15

4.3 TOE security objectives rationale 15

4.3.1 Security objectives rationale for the operational environment 16

5 Security Requirements 18

5.1 Overview 18

5.2 Security Functional Requirements 18

5.2.1 Overview 18

5.2.2 FCS_CKM.1 Cryptographic key generation 19

5.2.3 FCS_CKM.3 Cryptographic key access 20

5.2.4 FCS_CKM.6 Timing and event of cryptographic key destruction 20

5.2.5 FCS_RNG.1 Random number generation 20

5.2.6 FCS_COP.1 Cryptographic operation 21

5.2.7 FIA_ATD.1 User attribute definition 21

5.2.8 FIA_UAU.2 User authentication before any action 22

5.2.9 FIA_UID.2 User identification before any action 22
5.2.10 FMT_SMF.1 Specification of Management Functions 22
5.2.11 FMT_SMR.1 Security roles 25
5.2.12 FTP_TRP.1 Trusted path 25
5.3 TOE Security Assurance Requirements 25
5.4 Security Requirements Rationale 26
5.4.1 Dependency Rationale 26
6 TOE Summary Specification 29
6.1 Overview 29
6.2 Cryptographic Operation 29
6.3 Identification and Authentication 29
6.4 Security Management 30
6.5 Secure Communication 32

1 Security Target Introduction

1.1 ST Reference

ST Title	Meja Bulat Version 5.15.3 Security Target
ST Version	1.1
ST Date	24-JAN-2026

1.2 TOE Reference

TOE Title	Meja Bulat
TOE Version	5.15.3

1.3 Document Organization

This document is organized into the following major sections:

- Section 1 provides the introductory material for the ST as well as the TOE description
- Section 2 provides the conformance claims for the evaluation
- Section 3 provides the definition of the security problem that the TOE Operational Environment has been designed to address
- Section 4 defines the security objectives for the TOE operational environment
- Section 5 contains the security functional and assurance requirements derived from the Common Criteria, Part 2 and 3 respectively, which are in turn satisfied by the TOE and the development lifecycle
- Section 6 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE

1.4 Defined Terms

The following table defines all subjects, objects, operations, security attributes, external entities and other key terms that are used within the statements of security functional and assurance requirements. It also describes the acronym used in this documentation.

Term	Description
AES-GCM-256	AES (Advanced Encryption Standard) is a symmetric encryption algorithm used to turn readable data into unreadable data using a shared secret key. GCM (Galois/Counter Mode) is a method used with AES that adds integrity protection, ensuring the encrypted data has not been modified The 256-bit refers to the length of the encryption key
RAM	Random Access Memory
Remote Users	TOE users that interact indirectly with the TOE through another IT product. Example: For TOE user/TOE moderator to interact with the TOE web application, TOE user/TOE moderator has to use their workstation and web browser
SRTP	SRTP also known as Secure Real - Time Transport Protocol, is an extension profile of RTP (Real-Time Transport Protocol) which adds further security features, such as message authentication, confidentiality and replay protection mostly intended for Audio and Video communications.
System Administrator	System Administrator is an admin user who manages the system management console. System management console is an admin web page that is used by the System Administrator to manage TOE Moderator and TOE user. Note that System Administrator and system management console are out of the scope of evaluation
TOE	Target of Evaluation
TOE Moderator	Users that able to login to the TOE and access the TOE features stated in Table 5 – Management Functions
TOE User	Users that able to login to the TOE and access the TOE features stated in Table 5 – Management Functions
TSF	TOE Security Function
User data	Data created by and for the user, which does not affect the operation of the TSF.

1.5 TOE Overview

1.5.1 TOE Usage and Major Security Functions

The TOE is Meja Bulat Version 5.15.3. The TOE is a web application that is designed as a secure meeting platform and provides a protected environment for individuals and organizations to conduct virtual meetings, conferences, and collaborations. This platform prioritizes the safeguarding of sensitive information and privacy, offering a range of robust security features.

The TOE offers end-to-end encryption that ensures the content of a virtual meeting, such as audio, video, and chat messages, is encrypted at the source and can only be decrypted by the intended participants, providing a high level of security and privacy for the meeting's communications. End-to-end encryption, one of the hallmark elements, ensures that the content exchanged during a meeting remains private and secure. This means that only authorized participants possess the decryption keys, rendering the data inaccessible to potential eavesdroppers, including the platform provider. Additionally, user authentication, access controls, and password protection help prevent unauthorized access, guaranteeing that only invited participants can join the meeting. Furthermore, regular updates and compliance with industry regulations ensure that secure online meeting platforms stay ahead of emerging threats, making them a vital resource for organizations aiming to collaborate safely in a digital world.

The TOE offers a variety of features to facilitate effective communication and collaboration. Here is a list of common features:

- Video Conferencing: Support for video calls with multiple participants, including the ability to see and interact with each other through webcams.
- Audio Conferencing: High-quality audio calls, often with features like noise cancellation and the ability to mute/unmute participants.
- Screen Sharing: Share your screen with others to showcase presentations, documents, or software applications.
- Chat and Messaging: Real-time text chat for participants to exchange messages during the meeting.
- Recording: The ability to record meetings for later reference or sharing with absent participants.
- Virtual Backgrounds: The option to use virtual backgrounds or blur the background for privacy.

- Hand Raise and Reactions: Features that allow participants to signal when they want to speak or show agreement/disagreement.

- Participant Management: Hosts can mute/unmute participants, remove disruptive users, or manage permissions.

The TOE is designed with various security features and protocols to protect against unauthorized access, eavesdropping, data breaches, and other security threats. The following table highlights the range of security functions implemented by the TOE.

Security function	Description
Secure Communication	The TOE can protect the user data from disclosure and modification by using TLS v1.2 and SRTP (AES-GCM-256) as a secure communication
Cryptographic Support	The TOE implements encryption algorithm that utilize AES-GCM-256
Identification and authentication	The TOE requires that each user is successfully identified and authenticated before any interaction with protected resources is permitted. There are two types of users: TOE User and TOE Moderator. Please refer to Table 5 – Management Functions for the operations associated with each type of the users
Security Management	The TOE provides functions that allow management of the TOE and its security functions. The TOE restricts access to the management functions based on the role of the user.

1.5.2 TOE Type

The TOE is a secure meeting platform that provides protected end-to-end encryption. The TOE provides security functionality such as Secure Communication, Cryptographic Support, Identification and Authentication and Security Management. The TOE can be categorized as *Other Devices and Systems* in accordance with the categories identified in the Common Criteria Portal (www.commoncriteriaportal.org).

1.5.3 Supporting Hardware, Software and/or Firmware

The underlying hardware and software that is used to support the TOE are:

Minimum System Requirements	
Hardware and OS requirements for the server that will be hosting the TOE	
Processor	8 vCPUs
Operating System	Ubuntu 22.04
Memory (RAM)	16GB RAM

Storage	1 TB
Database	PostgreSQL 12,
Supporting Software	Docker (Web Hosting)
TOE Users Workstation	
Processor	11th Gen Intel(R)Core (TM) i7-1165G7 @ 2.80GHz
Operating System	Windows 10
Memory (RAM)	8GB RAM
Storage	500 GB
Web Browser	Microsoft Edge: 134 Mozilla Firefox: 136 Google Chrome: 134

1.6 TOE Description

1.6.1 Physical Scope of the TOE

A typical implementation of the TOE can be found in Figure 1 below, which identifies the various components of the TOE architecture.

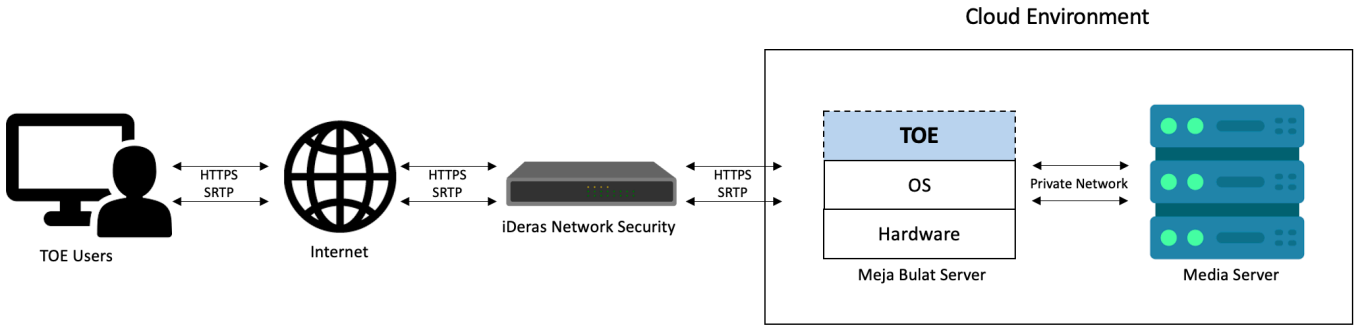

Figure 1 – TOE

Legend:

TOE Boundary

The TOE is a web application and is used by the TOE users and TOE moderator to perform operations stated in Table 5 – Management Functions. The primary access to the TOE is via a web application GUI by browsing to a link provided by the developer which is https://secure.infosysgateway.com.my. The TOE users and TOE moderator accessed the TOE via a supported web browser stated in Section 1.5.3

In order to perform the TOE operation, the TOE will need to communicate with several servers that are hosted locally in the developer environment which is located in Malaysia:

- Meja Bulat Server: Web Server is a server to host the TOE web application and system management console. System management console is a web based system used by the System Administrator to manage the TOE Moderators and TOE users. Note that System Administrator and system management console are out of the scope of evaluation

- Media Server: The Media Server is a PC that utilizes an Intel GPU and is connected to the internet via an Ethernet cable, which is also known as Ethernet Intel. The PC used for standby media server purposes is out of the scope of testing. This ready media server will act as a host if the TOE moderator who wants to host the meeting does not meet the media server requirement. Note that Media Server is out of the scope of evaluation.

If any issues occur, the customer or appointed account manager can communicate with the developer via the information provided below:

- Infosys Gateway Sdn. Bhd., Suite 3.02B, Level 3, South Wing, Menara OBYU, No. 4 Jalan PJU 8/8A, Damansara Perdana, 47820,Petaling Jaya, Selangor D.E, Malaysia

  Website: https://www.infosysgateway.com.my/support.html

  Email: info@infosysgateway.com.my

  Phone: +603-7732 9900

The TOE includes the following guidance documentation; Meja Bulat V5.15.3 Quick Guide PDF documentation

1.6.2 Logical Scope of the TOE

The logical boundary of the TOE is summarized below.

a) **Secure Communication.** The TOE provides a secure communication between the TOE and servers by utilizing HTTPS (TLS v1.2) and SRTP (AES-GCM-256)

b) **Cryptographic Support.** The TOE implements encryption algorithm that utilizes AES-GCM-256

c) **Identification & Authentication.** All users must be identified and authenticated before any information is permitted to flow. There are several login options on the login page:

   - Login using personal email: TOE Users need to input their personal email.

   - Login using Google account: TOE Users can sign in using their Google account.

- Login using Spotify account: TOE Users can access the TOE through their Spotify account.
- Login using X account: TOE Users can log in using their X account.
- Login as TOE moderator: The System Administrator registers the TOE user as a TOE moderator.

d) **Security Management.** The TOE contains various management functions to ensure efficient and secure management of the TOE users. The TOE maintains role-based access control mechanisms to ensure that functions are restricted to those who have the privilege to access them. The TOE provides a web-based interface that permits the TOE moderator user to manage the virtual meeting.

2 Conformance Claim

This ST and the TOE it describes are conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, CC:2022 Revision 1, November 2022.
    - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, CC:2022 Revision 1, November 2022.
    - Part 3 Conformant
- Common Criteria for Information Technology Security Evaluation Part 5: Pre-defined packages of security requirements, CC:2022 Revision 1, November 2022.

This ST and the TOE it describes are conformant to the following package:

- EAL1

3 Security Problem Definition

3.1 Overview

This section describes the nature of the security problem that the TOE operational environment is designed to address. The security problem is described through:

a) a series of ***threats*** that the TOE operational environment has been designed to mitigate,

b) specific ***assumptions*** about the security aspects of the environment (both IT related and non-IT related elements) in which the TOE will operate, and

c) any relevant ***organisational security policies*** statements that are made in terms of rules or guidelines that must be followed by the TOE and/or the operational environment.

3.2 Threats

Identifier	Threat statement
T.DISCLOSURE	An unauthorised user may attempt to compromise the integrity of the protected resource on the TOE

3.3 Organisational security policies

No organisational security policies have been defined regarding the use of the TOE.

3.4 Assumptions

Identifiers	Assumption statements
A.AUTHORISE	The TOE user and TOE moderator are not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the developer
A.OPSYS	The operating systems hosting the TOE components safeguard them from unauthorized access, modification, or deletion.
A.FIREWALL	The IT environment will implement gateway filtering; only allowing HTTP and HTTPS inbound connection traffic to pass through to TOE.
A.OS	The OS platforms on which the TOE operates is hardened to counter the perceived threats.

Identifiers	Assumption statements
A.TIMESTAMP	The platforms on which the TOE operates provides reliable timestamps
A.CRED	The TOE Moderator and TOE User will take appropriate measures to safeguard credentials employed for third-party authentication (such as X, Google, or Spotify), ensuring they are protected against potential threats and not exposed to unauthorized users.

4 Security objectives

4.1 Overview

The security objectives are a concise statement of the intended response to the security problem defined in Section 3.

4.2 Security objectives for the environment

Identifier	Objective statements
OE.AUTHORISE	The TOE user and TOE moderator assigned to operate the TOE is trusted by the organisation and are trained in use of the TOE.
OE.OPSYS	The operating systems that host the TOE components protect them from unauthorized access, modification, or deletion.
OE.FIREWALL	The IT environment implements gateway filtering; only allowing HTTP and HTTPS inbound connection traffic to pass through to Web server. The Web server would only accept service requests from the corresponding service provider. The TOE web and software application only accepts service requests from authorised service applications
OE.OS	The operating systems selected are of sufficient hardness to counter the perceived threats. The server-side hardness includes capabilities to establish a secure configuration to the OS, configure OS audit logs, configure proper OS authentication and permission, and ensure legacy services are not enabled.
OE.TIMESTAMP	Reliable timestamp is provided by the platform on which the TOE operate
OE.CRED	The TOE Moderator and TOE User must ensure that the credentials used for third-party authentication (such as X, Google, and Spotify) are secure, safeguarded against potential threats, and not exposed to unauthorized users.

4.3 TOE security objectives rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions and threats.

Table 1 - TOE Security Objectives Rationale

Objectives / Threats/ Assumptions	T.DISCLOSURE	A. AUTHORISE	A.OPSYS	A.FIREWALL	A.OS	A.TIMESTAMP	A.CRED
OE.AUTHORISE		✓					
OE.OPSYS	✓		✓		✓		
OE.FIREWALL				✓			
OE.OS			✓		✓		
OE.TIMESTAMP						✓	
OE.CRED							✓

4.3.1 Security objectives rationale for the operational environment

The following table demonstrates that all security objectives for the operational environment are trace back to assumptions in the security problem definition.

Table 2 - Security objectives rationale for the operational environment

Objectives	Assumption	Rationale
OE.AUTHORISE	A.AUTHORISE	OE.AUTHORISE fulfilled the assumption by ensuring the TOE user and TOE moderator assigned to operate the TOE is trusted by the organisation and are trained to use TOE and also download and install the TOE in accordance to the guidance document provided by the developer
OE.OS OE.OPSYS	A.OS A.OPSYS T.DISCLOSURE	OE.OS and OE.OPSYS fulfilled the assumptions by ensuring that operating systems selected are of sufficient hardness to counter the perceived threats and the operating system on the underlying platform meet the minimum requirements for the TOE and updated prior to installation to provide underlying security to the TOE.

Objectives	Assumption	Rationale
OE.FIREWALL	A.FIREWALL	OE.FIREWALL fulfilled the assumption by providing network filtering at the gateway through configuration of HTTPS and HTTP defined by the organization.
OE.TIMESTAMP	A.TIMESTAMP	OE.TIMESTAMP fulfilled the assumption by ensuring that reliable timestamps are provided by the operational environment for the TOE.
OE.CRED	A.CRED	OE.CRED fulfilled the assumption by ensuring that the TOE Moderator and TOE User secured and safeguarded the third-party authentication credentials (such as X, Google, and Spotify) against potential threats, ensuring they were not exposed to unauthorized users.

5 Security Requirements

5.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Revision 1, November 2022 providing functional requirements and part 3 providing assurance requirements.

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions used within this ST to depict their application:

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].

- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].

- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.

- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b.

5.2 Security Functional Requirements

5.2.1 Overview

The security functional requirements are expressed using the notation stated in Section 5.1 above and are itemised in the table below.

Identifier	Title
FCS_CKM.1	Cryptographic key generation
FCS_CKM.3	Cryptographic key access
FCS_CKM.6	Timing and event of cryptographic key destruction
FCS_RNG.1	Random number generation
FCS_COP.1	Cryptographic operation
FIA_ATD.1	User Attribute definition
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FTP_TRP.1	Trusted path

5.2.2 FCS_CKM.1 Cryptographic key generation

Hierarchical to:	No other components.
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**cryptographic key generation algorithms specified in Table 3 - Cryptographic Key Generation**] and specified cryptographic key sizes [**cryptographic key sizes specified in Table 3 - Cryptographic Key Generation**] that meet the following: [**standards as specified in Table 3 - Cryptographic Key Generation**]**.**
Dependencies	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] FCS_CKM.3 Cryptographic key access [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction
Notes:	

Table 3 - Cryptographic Key Generation

Algorithm	Key size (in bits)	Standard
AES-GCM-256	256	FIPS140

5.2.3 FCS_CKM.3 Cryptographic key access

Hierarchical to:	No other components.
FCS_CKM.3.1	The TSF shall perform [**key backup**] in accordance with a specified cryptographic key access method [**export to secure key vault**] that meets the following: [**none**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation or FCS_CKM.5 Cryptographic key derivation]
Notes:	None

5.2.4 FCS_CKM.6 Timing and event of cryptographic key destruction

Hierarchical to:	No other components.
FCS_CKM.6.1	The TSF shall destroy [**AES-GCM-256**] when [***no longer needed***].
FCS_CKM.6.2	The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method [**key deletion**] that meets the following: [**none**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation or FCS_CKM.5 Cryptographic key derivation]
Notes:	None

5.2.5 FCS_RNG.1 Random number generation

Hierarchical to:	No other components.

FCS_RNG.1.1	The TSF shall provide a [***deterministic***] random number generator that implements: [**generation of AES-GCM-256, cryptographic key generation, and nonce generation**].
FCS_RNG.1.2	The TSF shall provide [***bits***] that meet [**NIST SP 800-38D**].
Dependencies:	No dependencies.
Notes:	None

5.2.6 FCS_COP.1 Cryptographic operation

Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform [**cryptographic operations specified in Table 4 - Cryptographic Operation**] in accordance with a specified cryptographic algorithm [**cryptographic algorithm specified in Table 4 - Cryptographic Operation**] and cryptographic key sizes [**cryptographic key sizes specified in Table 4 - Cryptographic Operation**] that meet the following: [**standards as specified in Table 4 - Cryptographic Operation**]
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.3 Cryptographic key access
Notes:	**Table 4 - Cryptographic Operation** **Operation** | **Algorithm and mode** | **Key size (in bits)** | **Standard** Encryption and decryption | AES-GCM-256 | 256 | FIPS140

5.2.7 FIA_ATD.1 User attribute definition

Hierarchical to:	No other components
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**a. Username/Email,** **b. Password**].

Dependencies:	No dependencies
Notes:	None.

5.2.8 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.2.9 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	No dependencies.
Notes:	None.

5.2.10 FMT_SMF.1 Specification of Management Functions

<table>
<tr><td>Hierarchical to:</td><td>No other components.</td></tr>
<tr><td>FMT_SMF.1.1</td><td>The TSF shall be capable of performing the following management functions:
[Refer to Table 5 – Management Functions]
Table 5 – Management Functions
<table>
<tr><th>Subject</th><th>Object</th><th>Operation</th></tr>
<tr><td rowspan="5">TOE Moderator</td><td>Login</td><td>Login</td></tr>
<tr><td rowspan="3">Audio Settings</td><td>Mute/unmute</td></tr>
<tr><td>View/Edit Microphone</td></tr>
<tr><td>View/Edit Speakers</td></tr>
<tr><td rowspan="2">Video Settings</td><td>Start/Stop Camera</td></tr>
<tr><td>View/Edit Camera</td></tr>
</table>
</td></tr>
</table>

				View/Edit Virtual Background	
				Edit video mirroring	
			Screen Sharing	Start Screen Sharing End Screen Sharing	
			Chat	Open/Close Chat	
			Polls	Create/Cancel a poll	
			Hand	Raise/Lower Hand	
			Participants	Invite/Search Participant	
				Mute all	
				Disable all camera	
				Grant moderator rights	
				Kick out participant	
				Send private message	
				Add breakout room	
			More Action	Invite People	
				View/Edit Performance	
				View Full Screen	
				View/Edit Security Options	
				Start Recording End Recording	
				Share Video	
				Share Audio	
				Enable/Disable Noise Suppression	
				Show/Hide Whiteboard	
				View Participants statistics	
				View/Edit Settings	
			Hold	Hold/Unhold	

	Toggle	Toggle/Untoggle tile view	
TOE User	Login	Login	
	Audio Settings	Mute/unmute	
		View/Edit Microphone	
		View/Edit Speakers	
	Video Settings	Start/Stop Camera	
		View/Edit Camera	
		View/Edit Virtual Background	
		Edit video mirroring	
	Screen Sharing	Start Screen Sharing	
	Chat	Open/Close Chat	
	Polls	Create/Cancel a poll	
	Hand	Raise/Lower Hand	
	Participants	Invite/Search Participant	
		Send private message	
	More Action	Invite People	
		View/Edit Performance	
		View Full Screen	
		Start Recording	
		Share Video	
		Enable/Disable Noise Suppression	
		Show/Hide Whiteboard	
		View Participants stats	
		View/Edit Settings	
	Hold	Hold/Unhold	
	Toggle	Toggle/Untoggle tile view	

Dependencies:	No dependencies.
Notes:	None.

5.2.11 FMT_SMR.1 Security roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [**TOE User and TOE Moderator**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.2.12 FTP_TRP.1 Trusted path

Hierarchical to:	No other components.
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 or 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 [***initial user authentication***, [**and all further communication after authentication**]].
Dependencies:	No dependencies
Notes:	None.

5.3 TOE Security Assurance Requirements

EAL1 provides a basic level of assurance by a limited security target and an analysis of the SFRs in that ST using a functional and interface specification and guidance documentation, to understand the security behaviour. The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TSF. EAL1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents.

This EAL provides a meaningful increase in assurance over unevaluated IT.

Below are the assurance class and assurance components for EAL1:

Assurance class	Assurance components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing – conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

5.4 Security Requirements Rationale

5.4.1 Dependency Rationale

The table below demonstrates the mutual supportiveness of the SFRs for the TOE by demonstrating how the SFR dependencies are fulfilled by the TOE and by justifying those dependencies that are not fulfilled.

The SARs relevant to the TOE constitute an evaluation assurance level of EAL1, as defined in the Common Criteria and include no extensions or augmentations. Therefore, as a complete evaluation assurance level, they are a mutually supportive set and require no further justification.

SFR	Dependency	Inclusion
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] FCS_CKM.3 Cryptographic key access [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction	FCS_COP.1 FCS_CKM.3 FCS_RNG.1 FCS_CKM.6
FCS_CKM.3	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation or FCS_CKM.5 Cryptographic key derivation]	FCS_CKM.1
FCS_CKM.6	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation or FCS_CKM.5 Cryptographic key derivation]	FCS_CKM.1
FCS_RNG.1	No dependencies	N/A
FCS_COP.1	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.3 Cryptographic key access	FCS_CKM.1 FCS_CKM.3
FIA_ATD.1	No dependencies	N/A
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UID.2	No dependencies	N/A
FMT_SMF.1	No dependencies	N/A

SFR	Dependency	Inclusion
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2
FTP_TRP.1	No dependencies	N/A

6 TOE Summary Specification

6.1 Overview

This section provides the TOE summary specification, a high-level description of how the TOE implements the claimed security functional requirements. The TOE provides the following security functions:

- Cryptographic Support
- Identification and Authentication;
- Security Management; and
- Secure Communication

6.2 Cryptographic Operation

The TOE performs key generation, encryption and decryption using key size stated in Table 4 (**FCS_CKM.1, FCS_COP.1**). The TOE also able to destroy cryptographic keys by performing key deletion (**FCS_CKM.6**).

AES-GCM-256 is used by the TOE for end-to-end encryption **(FCS_COP.1)**. The key operation happens during the encryption and decryption

The TOE will execute key backup operations utilizing a specified cryptographic key access method, specifically exporting to a secure key vault. (**FCS_CKM.3**)

The TOE incorporates a deterministic random number generator designed to support critical cryptographic operations, including the generation of AES-GCM-256, cryptographic key generation, and nonce generation. Additionally, the TOE is required to generate random bits compliant with the standards specified in NIST SP 800-38D, ensuring robust and secure cryptographic processes (**FCS_RNG.1**)

6.3 Identification and Authentication

The TOE user and TOE moderator must provide authentication data to the TOE to affirm their identity and role prior to being granted access to any TOE functions or interfaces. Note that the TOE maintains two types of users which are TOE Moderator and TOE user (**FMT_SMR.1).** These users must be authenticated to the TOE prior performing any TOE functions by entering a valid email (for TOE user) / username (for TOE Moderator) and password (**FIA_ATD.1, FIA_UAU.2, FIA_UID.2).** To start utilizing the TOE, both users should visit the provided link (https://secure.infosysgateway.com.my/). Once on the TOE's homepage, they will find a variety of login options available.

- Log in using your personal email: To begin using TOE, TOE users must enter their personal email address. After doing so, they can click the 'Email me a one-time login link' button to receive a login link.
- Login using Google account: TOE Users can sign in using their Google account.
- Login using Spotify account: TOE Users can access the TOE through their Spotify account.
- Login using X account: TOE Users can log in using their X account.
- Login as TOE moderator: The System Administrator able to register the TOE user as a TOE Moderator in the the system management console. After registration, the TOE Moderator can log in by clicking the Login button. For a more detailed explanation on how to become a TOE Moderator, refer to the guidance document. System management console is an admin web page that is used by the System Administrator to manage TOE Moderator and TOE user. Note that System Administrator and system management console are out of the scope of evaluation.

6.4 Security Management

The TOE maintains two types of users which are TOE Moderator and TOE user (**FMT_SMR.1).** Below are the management function and users operation within the TOE **(FMT_SMF.1)**:

Subject	Object	Operation
TOE Moderator	Login	Login
	Audio Settings	Mute/unmute
		View/Edit Microphone
		View/Edit Speakers
	Video Settings	Start/Stop Camera
		View/Edit Camera
		View/Edit Virtual Background
		Edit video mirroring
	Screen Sharing	Start Screen Sharing End Screen Sharing
	Chat	Open/Close Chat
	Polls	Create/Cancel a poll

	Hand	Raise/Lower Hand
	Participants	Invite/Search Participant
		Mute all
		Disable all camera
		Grant moderator rights
		Kick out participant
		Send private message
		Add breakout room
	More Action	Invite People
		View/Edit Performance
		View Full Screen
		View/Edit Security Options
		Start Recording End Recording
		Share Video
		Share Audio
		Enable/Disable Noise Suppression
		Show/Hide Whiteboard
		View Participants statistics
		View/Edit Settings
	Hold	Hold/Unhold
	Toggle	Toggle/Untoggle tile view
TOE User	Login	Login
	Audio Settings	Mute/unmute
		View/Edit Microphone
		View/Edit Speakers
	Video Settings	Start/Stop Camera

		View/Edit Camera
		View/Edit Virtual Background
		Edit video mirroring
	Screen Sharing	Start Screen Sharing
	Chat	Open/Close Chat
	Polls	Create/Cancel a poll
	Hand	Raise/Lower Hand
	Participants	Invite/Search Participant
		Send private message
	More Action	Invite People
		View/Edit Performance
		View Full Screen
		Start Recording
		Share Video
		Enable/Disable Noise Suppression
		Show/Hide Whiteboard
		View Participants stats
		View/Edit Settings
	Hold	Hold/Unhold
	Toggle	Toggle/Untoggle tile view

6.5 Secure Communication

When a user (TOE user/TOE Moderator) accesses the TOE on their browser, by typing in the website address, the TOE will initiate a secure channel establishment with the user's browser (**FTP_TRP.1**). The TOE implements Transport Layer Security (TLS v1.2) secure communication protocol. The TOE also provides SRTP using AES-GCM-256 to encrypt and decrypt the messages.