IDOTTV Web Portal 2.0

Security Target

Version 1.11

Date: 17 January 2011

IDOTTV SDN. BHD.

Document History

Version No.	Date	Revision Description
1.0	24 May 2010	First initial release to evaluator
1.1	25 June 2010	Revised the TOE naming convention throughout the document. Added process flow in the logical scope. Revised TOE Overview. Took out T.DATA_CORRUPT. Redefined OE.INSTALL & OE.PHYSICAL. Mapped SFR's to Security Objectives. Revised existing SFR's and added new SFR's for audit log and https.
1.2	02 July 2010	Revised the document based on comments provided by evaluators on the 29th and 30th of June 2010 – revised the physical scope diagram, TOE security functions, threats, security objectives and other minor changes. Also, added more SFR's and changed the TOE reference.
1.3	06 July 2010	Reviewed and revised FDP_ACC.1. Added FAU_SAA.3 for SQL injection type of attack. Reviewed and revised non-TOE hardware and software. Reviewed and revised logical scope of the TOE as well as the TSS.
1.4	20 July 2010	Changed the ST title to not include "EAL 2" in section 2.1. Added OE.NETSEC for the requirement for a firewall for secure network configuration. Revised section 2.3.2 based on comments from evaluator.
1.5	04 August 2010	Took out the SFR for https and the relevant TSS section, and included the feature in the operational environment. Clarified the assignment in FAU_SAA.3 in the TSS section. Added the default session timeout to the TSS. Changed FMT_MTD.1 to only viewing of auditable data. Added rationale for SARs.
1.6	23 August 2010	Revised the SFR's based on comments in EOR1 dated 18 August 2010. Added description of administrators and users in the TOE Overview section.
1.7	24 November 2010	Revised the OSP and TSS based on comments from evaluator.
1.8	02 December 2010	Revised the figure in TOE physical scope, logical scope, and TSS.
1.9	11 December 2010	Added a security objective for the operational environment, OE.TRUSTEDCERT.
1.10	15 December 2010	Revised OE.NOEVIL, FAU_SAA.3, physical scope, logical scope and TSS>
1.11	17 January 2011	Revised the section 2.2.2 Hardware and Software Required by the TOE

TABLE OF CONTENTS

Page #

1 DOCUMENT INFORMATION

1.1 Document Conventions

The following conventions have been applied in this document:

Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: assignment, selection, and iteration.

1. The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold underline text**. Refinement for taking out a security requirement within the SFR's is denoted by ~~**bold strikethrough text**~~.
2. The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized text* in square brackets, [*selection value*].
3. The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment value].
4. The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration number).

1.2 Terminology

Acronym	Meaning
CC	Common Criteria
EAL	Evaluation Assurance Level
GB	Giga bytes
GHz	Giga Hertz
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
IDOTTV	IDOTTV Web Portal 2.0
IP	Internet Protocol. An Internet Protocol (IP) address is a numerical label that is assigned to devices participating in a computer network that uses the Internet Protocol for communication
LAN	Local Area Network
MB	Mega bytes
MHz	Mega Hertz
NTP	Network Time Protocol (a protocol used to synchronize the clocks of computers to some time reference)
PP	Protection Profile

Acronym	Meaning
RAM	Random Access Memory
SAR	Security Assurance Requirements
SFR	Security Functional Requirements
SQL	Structured Query Language
SSL	Secure Socket Layer or also known as Transport Layer Security (TLS)
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
TSS	TOE Summary Specification
URL	Uniform Resource Locator. The best-known example of a URL is the "address" of a web page on the World Wide Web.
User	Staff who uses the TOE
WAN	Wide Area Network

Table 1: Acronyms

1.3 References

- Common Criteria Part 1 Version 3.1 Revision 3
- Common Criteria Part 2 Version 3.1 Revision 3
- Common Criteria Part 3 Version 3.1 Revision 3
- Common Methodology for Information Technology Security Evaluation (CEM) version 3.1 Revision 3

1.4 Document Organization

This ST contains:

- TOE Description: Provides an overview of the TOE security functions and describes the physical and logical scope for the TOE.
- TOE Security Problem Definition: Describes the threats, organizational security policies, and assumptions that pertain to the TOE and the TOE environment.
- Security Objectives: Identifies the security objectives that are to be satisfied by the TOE and the TOE environment.
- TOE Security Functional Requirements: Presents the Security Functional Requirements (SFRs) met by the TOE.
- TOE Security Assurance Requirement: Presents the Security Assurance Requirements (SARs) met by the TOE.

- TOE Summary Specification: Describes the security functions provided by the TOE to satisfy the security requirements and objectives.
- TOE Rationale: Describes the rationale for threats and assumptions and mapping to the security objectives.

2 SECURITY TARGET INTRODUCTION

2.1 ST and TOE Reference

ST Title	IDOTTV Web Portal 2.0 Security Target
ST Version	Version 1.11
ST Publication Date	17 January 2010
TOE Identification	IDOTTV Web Portal 2.0
TOE Version	Version 2.0
CC Identification	CC Version 3.1 Revision 3
Assurance Level	EAL 2
ST Author	Ros Yusoff
Keywords	IDOTTV, Login Module

Table 2: TOE Reference

2.2 TOE Overview

IDOTTV Web Portal 2.0 is an online application system that enables users (of the system) to see the polling result and read SMS and MMS sent by public after reading the organization's published magazines. Users can either choose to view the results online or export to an excel spreadsheet format. Each user can only access to the polling result he / she is in charge of.

The application also allows editors (another group of authorized users) to publish tips or news to be sent to subscribers. Each editor has the access to his / her magazines only. He / She can only see the history of the tips or news he / she has sent to subscribers. There is another level of authorized users who can approve or reject the tips / news to be sent out to subscribers.

IDOTTV is an application to be used by an organisation with publications. Since it is web-based application, users and administrators can access the system and perform their task anywhere as long as there is an internet connection and they are authorized.

The scope of the TOE covers the following component of IDOTTV:

1. Web Portal for the authorized users and administrators

Note that administrators are those who handle administrative tasks of IDOTTV like creating, editing, and deleting users; setting user privileges; and, view audit trails. Users are those who operate the IDOTTV. For example, a user can be an editor who can publish tips or news.

The above scope of the TOE provides the following security features that are described in Section 2.3.2. Briefly, the security features introduced by the TOE are:

1. Security Audit
2. User Data Protection

3. Identification and authentication
4. Security management
5. TOE Access

2.2.1 TOE Type

IDOTTV Web Portal 2.0 is a web-based PHP application. The TOE is managed by authorized administrators through the web-based main page. Please refer to section 2.3.2 for the logical scope of the TOE.

2.2.2 Hardware and Software Required by the TOE

Below are the requirements for the hardware and software to run the TOE:

Servers:

The TOE is accessed via a web portal (for the authorized users and administrators) and installed on a computer that acts as a server, which has a minimum hardware, and software requirements as stated in the table below. The web portal and application systems are installed onto one physical server. And, the database component (which requires MySQL version 5.0.77) is installed onto another physical server.

No.	Requirement	Version / Specification
1	PHP Interpreter	PHP version 5.1.6
2	Apache Server	Apache version 2.2.3
3	Operating System	Windows Server 2003
4	Hardware	Xeon Quad Core, processor speed of 2.00 Ghz RAM of 4GB
5	Firewall	Any firewall devices as deemed appropriate by the organization

Table 3: Server Requirements

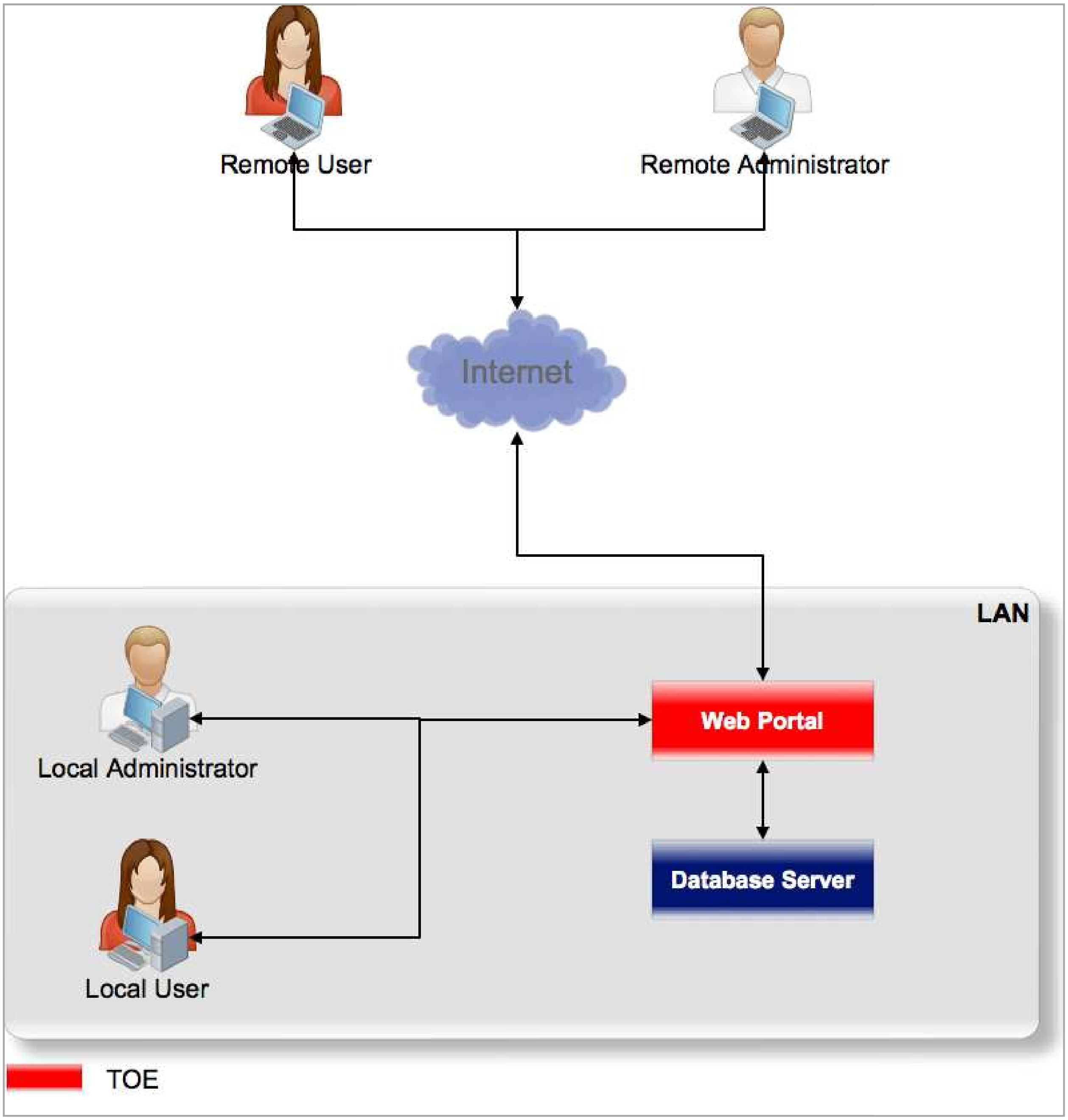
The client machine that is used by users and administrators requires a web browser of Internet Explorer 8 or Firefox 3.6.13.

Notes:

1. The mentioned hardware and software requirements are not part of the TOE.
2. All mentioned 3rd party software is not part of the TOE.

2.3 TOE Description

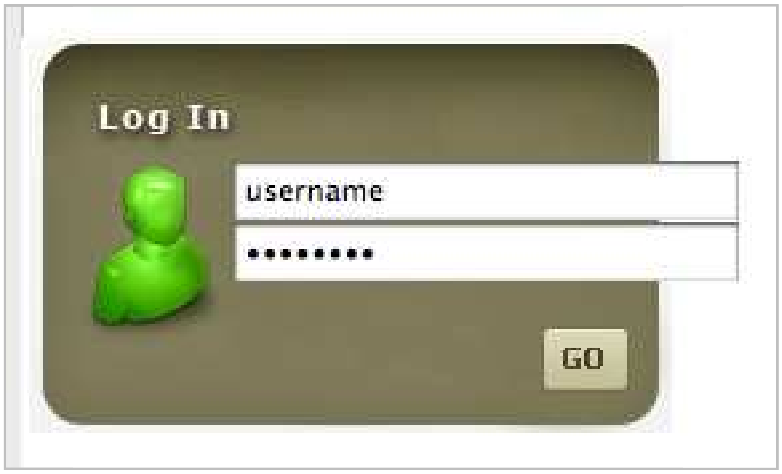
2.3.1 Physical Scope of the TOE



2.3.2 Logical Scope of the TOE

Below is the TOE scope description for the identified security functions. The details can be found in the TSS section.

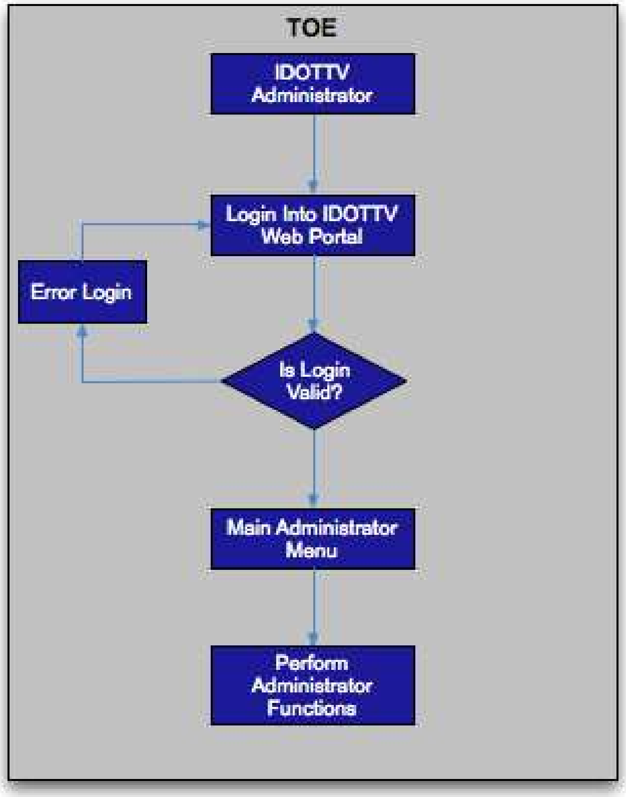
Security Function	TOE Scope Description
Security Audit	The TSF generates audit logs that consist of various auditable events or actions as listed in the table in section 7.1.1.1. Date and time of events, usernames, and events taken by the authorized users are recorded. Authorized administrators have the capability to read and view all the recorded logs stated above through the web portal. The TOE assumes that the operational environment provides a reliable time stamp source for the accuracy of the dates and times recorded in the logs mentioned above. Input validation checks are performed for selective fields within interactive forms within IDOTTV web portal for a protection against SQL injections. Refer to FAU_SAA.3 for the list of fields.
User Data Protection	Authorized administrators of the TOE can perform the following functions to the user or administrator accounts: 1. Account creation for users and additional administrators that includes the assignment of usernames and passwords 2. Access privilege assignments by user levels 3. Reset and unlock passwords for authorized users 4. Change password for own administrator

Security Function	TOE Scope Description
Identification and Authentication	The Identification and Authentication security function provides the TOE with the ability to govern access by users and administrators. An administrator can manage the TOE through the web portal (IDOTTV), a web-based graphical user interface. Prior to allowing access, the TOE requires an administrator to be identified using a username and password (alphanumeric). Before successful completion of the security function, an administrator is unable to perform any management function. Authorized users can access their relevant resources or functions once they have been successfully identified and authenticated using their usernames and passwords. Public data that is available on the main IDOTTV page in the Web Portal (which is not part of the TOE's scope) is accessible by everybody. 

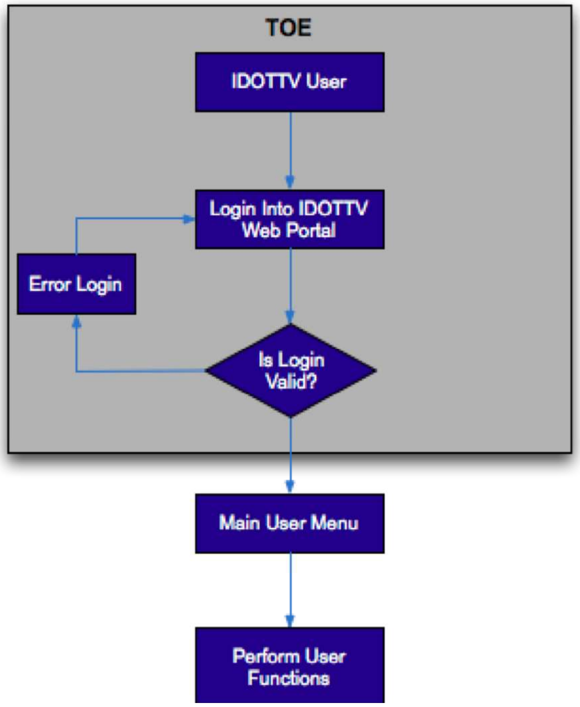
Security Function	TOE Scope Description
Security Management	The authorized administrators are able to create user accounts and assign them usernames and first time passwords for accessing the TOE. An administrator also has the ability to create other administrator accounts. At least one administrator is required to have full access rights to manage the TOE. Authorized administrators can assign access privileges to users by user levels based on the functions or resources that they are allowed to perform. Additional functionalities such as modifying access privileges and resetting / unlocking password for users are also accessible by authorized administrators.
TOE Access	Authorized administrators can define the session expiration time (in minutes). After inactivity of the specified period, the authorized users are then returned to the main page of the IDOTTV web portal. The TOE assumes that the operational environment of the IDOTTV web portal provides a reliable time stamp source. The TOE is able to deny session establishment once the session has expired. Re-authentication is required once the session ended.

Table 4: Logical Scope

Below is the process for administrators to log in to the web portal of IDOTTV.



Below is the process for users to log in to the web portal of IDOTTV.



3 CONFORMANCE CLAIMS

3.1 Common Criteria Claims

The following conformance claims are made for the TOE and ST:

- **CCv3.1 Rev.3 conformant**. The TOE and ST are Common Criteria conformant to Common Criteria version 3.1 Revision 3.
- **Part 2 extended**. The ST is Common Criteria Part 2 extended.
- **Part 3 conformant**. The ST is Common Criteria Part 3 conformant.
- The TOE and ST does not conform to **Protection Profiles**.

4 SECURITY PROBLEM DEFINITION

This section describes the security aspects of the environment in which the TOE will be used. It provides the statement of the TOE security environment that identifies:

- Known threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical and personnel aspects.

4.1 Threats to Security

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings/parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings/parameters and physical access to the TOE. (TOE users are assumed not to be willfully hostile to the TOE).

Both are assumed to have a low level of motivation. The IT assets requiring protection are the user data saved on or transitioning through the TOE and the hosts on the protected network. Mitigation of the threats is through the objectives identified in Section 4 - Security Objectives.

The following threats are applicable:

Threat Name	Description
T.UNAUTH	Users could gain unauthorized access to the TOE data by bypassing the identification and authentication requirements
T.DISCLOSE	Users could gain the passwords of authorized users and administrators by sniffing the traffic
T.INJECT	Users could inject a malicious code inserted into strings (through a SQL query) by inputting data from the forms available in the Web Portal

Table 5: Threats

4.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. It is assumed that organizations have their own organizational security policies.

4.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Assumption	Description
A.APP	It is assumed that the TOE and third party applications that the TOE relies upon have been configured in accordance with the installation guides. They are securely configured in such a way that the applications provide protection for the TOE from any unauthorized users or processes.
A.PROTECT	It is assumed that all hardware within the environment, including network and peripheral devices, has been approved for the transmitting of secured data. Each of these appliance configurations is securely managed by administrators to provide protection of secured data in terms of its confidentiality and integrity.
A.ADMIN	It is assumed that there are one or more competent individuals that are assigned to manage the TOE and its secured data. Such personnel are assumed not to be careless, willfully negligent or hostile.

Table 6: Assumptions

5 SECURITY OBJECTIVES

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 4). This section identifies the security objectives for the TOE and its supporting environment.

5.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Security Objective	Description
O.ADMIN	The TOE must provide a method for administrative control of the TOE
O.AUTH	The TOE must provide measures to uniquely identify and authenticate users prior to granting access to the functions or resources protected by the TOE
O.AUDIT	The TOE must record the login actions taken by users, prevent unauthorized deletion of the audit records stored on the TOE, and provide the authorized administrators with the ability to review the audit trail
O.VALIDATE	The TOE must validate input from users and administrators based on type, length, format and range.

Table 7: Security Objectives for the TOE

5.2 Security Objective for the Operational Environment

Certain objectives with respect to the general operating environment must be met for the TOE to meet its security functional requirements. Those objectives are:

Security Objective	Description
OE.NOEVIL	Administrators and Users are non-hostile, appropriately trained, and follow all user guidance, installation guidance and configuration guidance. The Administrators and users must ensure the physical security of the computers that they use to connect to the TOE to prevent cookie stealing.
OE.INSTALL	Those responsible for the TOE must ensure that the TOE and third party software are delivered, installed, managed, and operated in a manner which maintains the organizational IT security objectives.
OE.RELIABLE	All hardware and third party software supporting the TOE are reliable and operating in good condition. All supporting third party software must be updated with services packs, fixes, patches and anti-virus patterns. All supporting components' performance is

Security Objective	Description
	monitored and maintained by administrators.
OE.PHYSICAL	The operational environment of the TOE restricts the physical access to the TOE and non-TOE (hardware and software) to administrative personnel and maintenance personnel accompanied by administrative personnel.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials, such as passwords or other authentication information, are protected by the users (by complying with organizational policies and procedures disallowing disclosure of user credential information) in a manner which maintains organizational IT security objectives.
OE.NETSEC	The operational environment of the TOE must include a firewall that is configured securely to permit or deny traffic based upon a set of rules. The administrative personnel must configure the firewall rules to block unauthorized access while permitting authorized communications.
OE.CHANNEL	The operational environment of the TOE must protect the transmitted passwords to the Web Portal via usage of HTTPS using a server based SSL.
OE.TRUSTEDCERT	The users (or administrators) of the TOE will be alerted if the certificate used for establishing the HTTPS session is not the right (or trusted) server certificate. If this happens, users (or administrators) are not to trust the server certificate.

Table 8: Security Objective for the Operational Environment

5.3 RATIONALE

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the ST. Sections 5.3.1, 5.3.2, and 5.3.3 demonstrate the mappings between the threats, polices, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

5.3.1 Security Objectives Rationale Relating to Threats

Threats	Objectives	Rationale
T.UNAUTH Users could gain unauthorized access to the TOE data by bypassing the identification and authentication requirements	O.ADMIN The TOE must provide a method for administrative control of the TOE	O.ADMIN mitigates this threat by ensuring that a session with user inactivity for a period of time specified by the administrators will be logged out. Once they are logged out, re-identification and re-authentication is required. (no bypass is allowed).
	O.AUTH	O.AUTH mitigates this threat by ensuring that only authorized users

Threats	Objectives	Rationale
	The TOE must provide measures to uniquely identify and authenticate users prior to granting access to the functions or resources protected by the TOE.	with valid usernames and passwords can access the functions or resources protected by the TOE.
	OE.CREDEN Those responsible for the TOE must ensure that all access credentials, such as passwords or other authentication information, are protected by the users (by complying with policies and procedures disallowing disclosure of user credential information) in a manner which maintains IT security objectives.	OE.CREDEN mitigates this threat by ensuring that all user credentials are protected appropriately by users.
	O.AUDIT The TOE must record the login actions taken by users, prevent unauthorized deletion of the audit records stored on the TOE, and provide the authorized administrators with the ability to review the audit trail.	O.AUDIT ensures that events of security relevance as in the table of auditable events in section 7.1.1.1 are audited to enable administrators to review suspicious login activities. It also ensures that only authorized administrators can view the audit data.
T.DISCLOSE Users could gain the passwords of authorized users and administrators by sniffing the traffic	OE.CHANNEL The operational environment of the TOE must protect the transmitted passwords to the Web Portal via usage of HTTPS using a server based SSL.	OE.CHANNEL mitigates this threat by protecting the passwords transmitted. The communication path between the Web Portal and remote users / administrators is via a trusted https tunnel using SSL/TLS.
	OE.TRUSTEDCERT The users (or administrators) of the TOE will be alerted if the certificate used for establishing the HTTPS session is not the right (or trusted) server certificate. If this happens, users (or administrators) are not to trust the server certificate.	OE.TRUSTEDCERT mitigates this threat by ensuring that users (or administrators) do not trust a non-trusted server certificate. The users (or administrators) will be alerted if the certificate used for establishing the HTTPS session is not the right (or trusted) server certificate.
T.INJECT Users could inject a malicious code inserted into strings (through a SQL query) by inputting data from the forms available in the Web Portal	O.VALIDATE The TOE must validate input from users and administrators based on type, length, format and range	O.VALIDATE mitigates this threat by enforcing the TSF to perform input validation on all fields available for users and administrators in the Web Portal.

Table 9: Mapping of Threats and Objectives

Every threat is mapped to one or more objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

5.3.2 Security Objectives Rationale Relating to Policies

There are no policies defined for this Security Target.

5.3.3 Security Objectives Rationale Relating to Assumptions

Assumptions	Objectives	Rationale
A.APP It is assumed that the third party applications that the TOE relies upon have been configured in accordance with the installation guides. They are securely configured in such a way that the applications provide protection for the TOE from any unauthorized users or processes	OE.RELIABLE All hardware and third party software supporting the TOE are reliable and operating in good condition. All supporting third party software must be updated with services packs, fixes, patches and anti-virus patterns. All supporting components' performance is monitored and maintained by administrators	OE.RELIABLE satisfies this assumption by ensuring that all hardware and software used are reliable and they are in good condition. Their performances are also monitored and maintained by the organization
	OE.INSTALL Those responsible for the TOE must ensure that the TOE and third party software are delivered, installed, managed, and operated in a manner which maintains organizational IT security objectives.	OE.INSTALL satisfies this assumption by ensuring that the installation and configuration of the TOE and third party software are performed in a manner that maintain security objective of the organization. The TOE and third party software installation and configuration are performed by the developer of the application system.
A.PROTECT It is assumed that all hardware within the environment, including network and peripheral devices, has been approved for the transmitting of secured data. Each of these appliance configurations is securely managed by administrators to provide protection of secured data in terms of its confidentiality and integrity.	OE.PHYSICAL The operational environment of the TOE restricts the physical access to the TOE and non-TOE (hardware and software) to administrative personnel and maintenance personnel accompanied by administrative personnel.	OE.PHYSICAL satisfies this assumption by assuming that physical security is provided where the access to the servers are controlled
	OE.INSTALL Those responsible for the TOE must ensure that the TOE and third party software are delivered, installed, managed, and operated in a manner which maintains organizational IT security objectives.	OE.INSTALL satisfies this assumption by ensuring that the installation and configuration of the TOE and third party software are performed in a manner that maintain security objective of the organization. The TOE and third party software installation and configuration are performed by the developer of the application system.
	OE.NOEVIL Administrators and Users are non-hostile, appropriately trained, and follow all user guidance, installation guidance and configuration guidance. The Administrators and users must ensure the physical security of the computers that they use to connect to the TOE to prevent cookie stealing.	OE.NOEVIL satisfies this assumption by ensuring that administrators and users are non-hostile and appropriate trained. It also satisfies this assumption by ensuring the physical security of the computers used to connect to the TOE to prevent cookie stealing.
	OE. NETSEC The operational environment of the TOE must include a firewall that is configured securely to permit or deny traffic based upon a set of rules. The administrative	OE.NETSEC satisfies this assumption by ensuring that there exists a firewall that has been configured to block unauthorized access while permitting authorized communications.

Assumptions	Objectives	Rationale
	personnel must configure the firewall rules to block unauthorized access while permitting authorized communications.	
A.ADMIN It is assumed that there are one or more competent individuals that are assigned to manage the TOE and its secured data. Such personnel are assumed not to be careless, willfully negligent or hostile.	OE.NOEVIL Administrators and Users are non-hostile, appropriately trained, and follow all user guidance, installation guidance and configuration guidance. The Administrators and users must ensure the physical security of the computers that they use to connect to the TOE to prevent cookie stealing.	OE.NOEVIL satisfies this assumption by ensuring that administrators and users are non-hostile and appropriate trained. It also satisfies this assumption by ensuring the physical security of the computers used to connect to the TOE to prevent cookie stealing.
	OE.CREDEN Those responsible for the TOE must ensure that all access credentials, such as passwords or other authentication information, are protected by the users (by complying with organizational policies and procedures disallowing disclosure of user credential information) in a manner which maintains organizational IT security objectives.	OE.CREDEN satisfies this assumption by ensuring that all user credentials are protected appropriately by users and they are not negligent

Table 10: Mapping of Assumptions and Objectives

6 EXTENDED COMPONENTS

6.1 Extended Components Definition

The table below contains the extended security functional requirements for the TOE:

Security Function Class	Security Function Component
FPT: Protection of the TSF	FPT_STM_EXT.1 Reliable time stamps

Table 11: Extended Component

FPT class contains families of functional requirements that relate to the integrity and management of the mechanisms that constitute the TSF and to the integrity of TSF data.

The above component is a member of FPT_STM, an existing CC Part 2 family. The following extended requirement for the FPT class has been included in this ST because the operational environment is capable of providing reliable time stamps for TSF functions that is not covered in CC Part 2.

Reliable time stamps (FPT_STM_EXT.1)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM_EXT.1.1: The operational environment shall be able to provide reliable time stamps for the TSF functions.

Application Note: *Reliable Time Stamps is required for the TOE to capture date and time events in relations to the FAU_GEN.1 and FMT_SAE.1 security functions. The TOE does not have a feature to generate time stamps independently. The underlying operating system needs to provide reliable time stamps from the system clock for use by the TOE. The date and time stamps provided by the underlying operating system can be manually configured by administrators or fed by NTP servers.*

6.2 Rationale for Extended Security Functional Requirements

FPT_STM.1:

FPT_STM.1 is a dependency of FAU_GEN.1 and FMT_SAE.1 that have not been included. Reliable time stamps are provided by the operational environment through an interface of the TOE. The time stamps captured in the TOE is derived from the operating system of the computer on which the instance of IDOTTV web portal is installed and running.

7 SECURITY REQUIREMENTS

This section specifies the requirements for the TOE.

7.1 TOE Security Functional Requirements (SFRs)

This section specifies the SFRs for the TOE. It organizes the SFRs by the CC classes.

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1; Audit data generation
	FAU_SAA.3: Simple attack heuristics
	FAU_SAR.1: Audit review
	FAU_STG.1: Protected audit trail storage
FDP: User Data Protection	FDP_ACC.1: Subset access control
	FDP_ACF.1: Security attribute based access control
FIA: Identification and Authentication	FIA_ATD.1: User attribute definition
	FIA_UAU.1: Timing of authentication
	FIA_UID.1: Timing of identification
FMT: Security Management	FMT_MSA.1: Management of security attributes
	FMT_MSA.3: Static attribute initialisation
	FMT_MTD.1: Management of TSF data
	FMT_SAE.1: Time-limited authorization
	FMT_SMF.1: Specification of management functions
	FMT_SMR.1: Security Roles
FTA: TOE Access	FTA_LSA.1: Limitation on scope of selectable attributes
	FTA_SSL.3: TSF-initiated termination
	FTA_TSE.1: TOE session establishment

Table 12: TOE Security Functional Requirements

7.1.1 Security Audit

7.1.1.1 Audit Data Generation (FAU_GEN.1)

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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) [all auditable events – refer to table below].

Auditable Events
User log in
User Log out
Failed login attempts
Password changed successfully
Add user successful
Delete user successful

Table 13: Auditable Events

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, outcome (success or failure) of the event; and
b) For audit event type, based on the auditable event definitions of the functional components included in the ST, [none].

Application Note: *Please refer to Section 6.2 for the rationale for not addressing the FPT_STM.1 as a dependency of FAU_GEN.1.*
The TOE is more restrictive as it does not allow the administrators or users to start-up and shutdown the audit functions. The audit functions are always on.

7.1.1.2 Simple Attack Heuristics (FAU_SAA.3)

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAA.3.1 The TSF shall be able to maintain an internal representation of the following signature events [SQL injections] that may indicate a violation of the enforcement of the SFRs.

FAU_SAA.3.2 The TSF shall be able to compare the signature events against the record of system activity discernible from an examination of [inputs by validating data in the specified fields (as listed in the Application Note below) in the Web Portal].

FAU_SAA.3.3 The TSF shall be able to indicate a potential violation of the enforcement of the SFRs when a system event is found to match a signature event that indicates a potential violation of the enforcement of the SFRs.

Application Note: *The fields where input validation is performed are:*

1. *Username*
2. *Password*
3. *Staff Number*
4. *Phone Number*
5. *Mobile Number*
6. *Fax Number*

7.1.1.3 Audit Review (FAU_SAR.1)

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit Data Generation

FAU_SAR.1.1 The TSF shall provide [authorized administrators] with the capability to read [all recorded audit information] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

7.1.1.4 Protected Audit Trail Storage (FAU_STG.1)

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit Data Generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [*prevent*] unauthorized modifications to the stored audit records in the audit trail.

7.1.2 User Data Protection

7.1.2.1 Subset Access Control (FDP_ACC.1)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [administrator access control SFP] on [administrators performing the following operations (or management functions) to the user and administrator accounts:

a) account creation for users and additional administrators that includes the assignment of usernames and passwords
b) access privilege assignments by user levels

c) reset and unlock passwords for authorized users
d) change password for own administrator account].

7.1.2.2 Security attribute based access control (FDP_ACF.1)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset Access Control
FMT_MSA.3 Static Attribute Initialization

FDP_ACF.1.1 The TSF shall enforce the [administrator access control SFP] to objects based on the following: [Usernames and user groups].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [users are explicitly granted access to a function or resource if he/she belongs to a user group which has been granted access].

FDP_ACF.1.3 The TSF shall explicitly authorize 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].

7.1.3 Identification and Authentication

7.1.3.1 User attributes definition (FIA_ATD.1)

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1: The TSF shall maintain the following list of security attributes belonging to individual users: [

a) Username and password
b) User group or role].

7.1.3.2 Timing of authentication (FIA_UAU.1)

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1: The TSF shall allow [read access to public objects] 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.

7.1.3.3 Timing of identification (FIA_UID.1)

Hierarchical to: No other components.

Dependencies:	No dependencies.
FIA_UID.1.1:	The TSF shall allow [read access to public objects] 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.

7.1.4 Security Management

7.1.4.1 Management of security attributes (FMT_MSA.1)

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions
FMT_MSA.1.1:	The TSF shall enforce the [administrator access control SFP] to [*reset or unlock*] the security attributes [passwords] to [authorized administrators].

7.1.4.2 Static attribute initialisation (FMT_MSA.3)

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1:	The TSF shall enforce the [administrator access control SFP] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2:	The TSF shall allow the [authorized administrators] to specify alternative initial values to override the default values when an object or information is created.

7.1.4.3 Management of TSF data (FMT_MTD.1)

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of management functions
FMT_MTD.1.1:	The TSF shall restrict the ability to [*view*] the [auditable datas defined in Tabe 13 above] to [authorized administrators].

7.1.4.4 Time-limited authorisation (FMT_SAE.1)

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FPT_STM.1 Reliable time stamps

FMT_SAE.1.1: The TSF shall restrict the capability to specify an expiration time for [authorized user authentication data in the web portal] to [authorized administrators].

FMT_SAE.1.2: For each of these security attributes, the TSF shall be able to [log out the associated authorized user account for the web portal] after the expiration time for the indicated security attribute has passed.

Application Note: *Please refer to Section 6.2 for the rationale for not addressing the FPT_STM.1 as a dependency of FMT_SAE.1.*

7.1.4.5 Specification of management functions (FMT_SMF.1)

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1: The TSF shall be capable of performing the following management functions: [

a) account creation for users and additional administrators that includes the assignment of usernames and passwords
b) access privilege assignments by user levels
c) viewing of audit data
d) reset and unlock passwords for authorized users
e) change password for own administrator account].

7.1.4.6 Security roles (FMT_SMR.1)

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1: The TSF shall maintain the roles [authorized users and administrators].

FMT_SMR.1.2: The TSF shall be able to associate users with roles.

7.1.5 TOE Access

7.1.5.1 Limitation on scope of selectable attributes (FTA_LSA.1)

Hierarchical to: No other components

Dependencies: No dependencies

FTA_LSA.1.1 The TSF shall restrict the scope of the session security attributes [session timeout], based on [user inactivity].

7.1.5.2 TSF-initiated Termination (FTA_SSL.3)

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1: The TSF shall terminate an interactive session after [a logout or a specified time interval of user inactivity set by an authorized administrator. The default session timeout value is 15 minutes].

7.1.5.3 TOE session establishment (FTA_TSE.1)

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TSE.1.1: The TSF shall be able to deny session establishment based on [session timeout for the authorised users and administrators].

7.2 TOE Security Assurance Requirement

The TOE meets the security assurance requirements for EAL2. The following table is the summary for the requirements:

ASSURANCE CLASS	ASSURANCE COMPONENTS
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

Table 14: TOE Security Assurance Requirements

7.2.1 Rationale for Security Assurance Requirements (SARs)

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software development practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. The threats that were chosen are consistent with attacker of low attack motivation, therefore EAL2 was chosen for this ST.

8 TOE SUMMARY SPECIFICATION

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST. Each of the security requirements and the associated descriptions correspond to the security functions. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

8.1 TOE Security Functions

8.1.1 Security Audit

Users and administrators access the TOE through the IDOTTV web portal. The TOE generates audit logs that consist of various auditable events or actions taken by the users and administrators (as listed in the table in section 7.1.1.1). The auditable events include user logins, user logouts, failed login attempts, password changes, creation of users or administrators, and deletion of users or administrators. The audit contents consist of the date and time of events, usernames, and events taken by the authorized users or administrators. These audit logs can be analyzed by authorized administrators for suspicious activities, when required.

The TOE provides the capability for authorized administrators to read and view all the recorded logs stated above through the web portal. Note that only the administrators can view the audit log. The TSF prevents the authorized administrators from modifying or deleting audit logs.

The TOE assumes that the operational environment provides a reliable time stamp source for the accuracy of the dates and times recorded in the logs mentioned above.

Not validating input is one of the reasons for malicious database manipulation or system crashes. User Data Protection function provides the TSF with the ability to protect user data by ensuring data sent to the Web Portal is validated prior to processing it.

All input to the specified fields available in selective interactive forms in the IDOTTV Web Portal is validated before it is processed. The input is validated based on size of the input, the sequence of the keystroke, and the list of unacceptable characters (knowns as “black” list) to ensure that no malicious code is inserted into the SQL query or at least keep malicious code from being processed.

Functional Requirement Satisfied: FAU_GEN.1, FAU_SAR.1, FAU_STG.1, FMT_MTD.1, FPT_STM_EXT.1, FAU_SAA.3.

8.1.2 User Data Protection

Authorized administrators of the TOE can perform the following functions to the user or administrator accounts:

5. Account creation for users and additional administrators that includes the assignment of usernames and passwords
6. Access privilege assignments by user levels
7. Reset and unlock passwords for authorized users
8. Change password for own administrator

Users (and administrators) can only access resources (or functions) if they belong to the user group that explicitly have been given access to those resources or functions. Only administrators can give perform the user access privileges.

Functional Requirement Satisfied: FDP_ACC.1, FDP_ACF.1

8.1.3 Identification and Authentication

The Identification and Authentication security function provides the TOE with the ability to govern access by users and administrators. The TOE ensures that a user (or administrator) identity is established and verified before access to the TOE is allowed. The identity (which is the username) is associated to its proper user group.

An administrator can manage the TOE through the web portal (IDOTTV), a web-based graphical user interface. Prior to allowing access, the TOE requires an administrator to be identified using a username and password (must be alphanumeric). Before successful completion of the security function, an administrator is unable to perform any of the management function.

Users of the TOE must be identified and authenticate prior accessing the functions or resources the web portal (IDOTTV). Before successful completion of the security function, a user is unable to perform any of the relevant function.

Public data that is available on the main IDOTTV page with the Web Portal (which is not part of the TOE's scope) is accessible by everybody. Once identified and authenticated, the users and administrators are able to access the functions or resources available to their respective groups' access levels.

TOE Security Functional Requirements Satisfied: FIA_ATD.1, FIA_UAU.1, FIA_UID.1,

8.1.4 Security Management

The purpose of the TOE is provide services to users to publish tips or news and view polling results, as well as other services specified in section 2.2 in the TOE Overview. The TOE provides mechanisms to govern which users can access with resources or functions. The Security Management function allows the administrators to properly configure this functionality.

The authorized administrators can manage user accounts where they are able to create user accounts and assign them usernames and passwords for accessing the TOE. An administrator also has the ability to create other administrator accounts. At least one administrator is required to have full access rights to manage the TOE. The restrictive default password for a new user or administrator created is "ABC123". This password will then need to be changed by the administrator or user when they first login to the system.

Authorized administrators can assign access privileges to users by user levels based on the functions or resources that they are allowed to perform or access. Additional functionality such as modifying access privileges is also accessible by authorized administrators. Authorized administrators are also able to reset (reset to default of "ABC123") the passwords for users by overriding the passwords (the administrator can choose to notify the user of the default password manually), as well as unlocking passwords for users.

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

8.1.5 TOE Access

The TSF provides a method for controlling the establishment of a user's (or administrator's) session based on a termination of session after a specified period of user inactivity.

Authorized administrators can define the session expiration time (in minutes) for authorized users and administrators. Inactive sessions are logged out after this defined period of inactivity. The users are automatically logged out and returned to the login page. The default session timeout is 15 minutes.

The TOE is able to deny session establishment once the session has expired. Re-authentication is required once the session ended.

The TOE assumes that the operational environment provides a reliable time stamp source.

TOE Security Functional Requirements Satisfied: FMT_SAE.1, FTA_LSA.1, FTA_SSL.3, FTA_TSE.1, FPT_STM_EXT.1.

8.2 Rationale for SFR's of the TOE Objectives

Objective	SFR's Addressing the Objective	Rationale
O.ADMIN The TOE must provide a method for administrative control of the TOE.	FMT_MSA.1: Management of security attributes	FMT_MSA.1 specifies that only authorized administrators can reset and unlock passwords for authorized users
	FMT_MSA.3: Static attribute initialization	FMT_MSA.3 specifies that authorized administrators can override the values of objects like passwords or session timeout
	FMT_SAE.1: Time-limited authorization	FMT_SAE.1 specifies the TSF to restrict an expiration time for user inactivity
	FMT_SMF.1: Specification of management functions	FMT_SMF.1 specifies the management functions the TOE must provide.
	FMT_SMR.1: Security Roles	FMT_SMR.1 requires the TOE to maintain user and administrator roles.
	FTA_LSA.1: Limitation on scope of selectable attributes	FTA_LSA.1 requires the TSF to restrict the session timeout based on user inactivity
	FTA_SSL.3: TSF-initiated termination	FTA_SSL.3 requires the TSF to terminate an interactive session after a specified time interval of user inactivity that is set by authorized administrators
	FPT_STM_EXT.1: Reliable time stamps	FPT_STM_EXT.1 requires that the operating systems (in which the web portal is installed and running) provide reliable time stamps to be used in FMT_SAE.1.
O.AUTH	FDP_ACC.1: Subset access	FDP_ACC.1 specifies the TSF to

Objective	SFR's Addressing the Objective	Rationale
The TOE must provide measures to uniquely identify and authenticate users prior to granting access to the functions or resources protected by the TOE	control	enforce the user privileges based on the usernames and user groups (associated to those usernames). Users are granted access to functions or resources if they belong to user groups that have been granted access.
	FDP_ACF.1: Security attribute based access control	FDP_ACC.1 specifies the TSF to enforce administrator access control on the management functions.
	FIA_ATD.1: User attribute definition	FIA_ATD.1 requires that the TSF maintain the usernames and passwords, as well as the functions those users or administrators are allowed to access.
	FIA_UAU.1: Timing of authentication	FIA_UAU.1 requires that users and administrators be authenticated before allowing access to TSF-mediated actions that are relevant to those users and administrators.
	FIA_UID.1: Timing of identification	FIA_UID.1 requires that users and administrators be identified before allowing access to TSF-mediated actions that are relevant to those users and administrators.
	FTA_TSE.1: TOE session establishment	FTA_TSE.1 requires the TSF to deny a session establishment once the session has timed out (based on user inactivity)
O.AUDIT The TOE must record the login actions taken by users, prevent unauthorized deletion of the audit records stored on the TOE, and provide the authorized administrators with the ability to review the audit trail.	FAU_GEN.1; Audit data generation	FAU_GEN.1 defines the basic auditable events to be recorded as listed in Table 13.
	FAU_SAR.1: Audit review	FAU_SAR.1 defines the capability of authorized administrators to read the audit records as listed in Table 13.
	FAU_STG.1: Protected audit trail storage	FAU_STAG.1 defines that audited records as listed in Table 13 are protected (only authorized administrators can view the records).
	FMT_MTD.1: Management of TSF data	FMT_MTD.1 defines that the audit log can only be viewed by an authorized administrator.
	FPT_STM_EXT.1: Reliable time stamps	FPT_STM_EXT.1 requires that the operating systems (in which the web portal is installed and running) provide reliable time stamps to be used in FAU_GEN.1.
O.VALIDATE The TOE must validate input from users and administrators based on type, length, format and range	FAU_SAA.3: Simple attack heuristics	FAU_SAA.3 specifies the TSF to enforce input validation on data input in selective fields in the Web Portal.

Table 15: Mapping of SFR's and Objectives