Metastorm e-Work 6.6.1 Security Target

Version 1.0

2006/10/03

Prepared for:
Metastorm, Inc.

8825 Stanford Blvd
Suite 200
Columbia, MD 21045

Prepared By:
Science Applications International Corporation

Common Criteria Testing Laboratory

7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is Metastorm e-Work 6.6 provided by Metastorm, Inc.. The TOE provides the ability to view and manage information, activities, and instructions that can be used to automate a business process, for example a manager approving a staff member's form for a travel request form.

The Security Target contains the following additional sections:

- TOE Description (Section 2): This section gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE.
- Security Environment (Section 3): This section details the expectations of the environment,. Describing the threat, mitigate assumptions and the organizational security polices and the TOE and its environment must adhere to.
- Security Objectives (Section 4): This section details the security objectives of the TOE and its environment.
- IT Security Requirements (Section 5): The section presents the security functional requirements (SFR) for TOE and IT Environment that supports the TOE, and details the requirements for EAL 2.
- TOE Summary Specification (Section 6): The section describes the security functions represented in the TOE that satisfies the security requirements.
- Protection Profile Claims (Section 7): This section identifies the Protection Profile Claim made in the ST.
- Rationale (Section 8): This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – Metastorm e-Work 6.6 Security Target

ST Version – Version 1.0

ST Date – 2006/10/03

TOE Identification – Metastorm e-Work 6.6.1

TOE Developer – Metastorm Incorporated

Evaluation Sponsor – Metastorm Incorporated

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.2, Revision 256, January 2004.

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.2, Revision 256, January 2004.
    - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.2, Revision 256, January 2004.

- Part 3 Conformant
- Assurance Level: EAL 2
- Strength of Function Claim: SOF-basic

1.3 Conventions, Terminology, Acronyms

This section specifies the formatting information used in the Security Target.

1.3.1 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: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.
- Explicitly stated requirements – Security Functional Requirements not defined in Part 2 of the CC are annotated with EX.

2. TOE Description

The Target of Evaluation (TOE) is Metastorm e-Work 6.6.1.

The TOE is an IT enabled Business Process Management (BPM) software product supported on Windows 2003, NT, 2000, and XP. The TOE manages and tracks business processes flow and data in real time.

The TOE is a subset of the product. Individual product components that are included in the evaluated configuration are identified and described below.

The remainder of this section summarizes the Metastorm architecture.

2.1 TOE Overview

The TOE is an IT enabled Business Process Management (BPM) software product supported on Windows 2003, 2000, and XP. BPM is the process of viewing and managing the information, activities, and instructions required to automate a business process which is called a procedure. The main component of a procedure is one or more maps. Maps are diagrams or process model logical constructs that depict business processes such as a manager approving a staff member's form for a travel request form, for example.

2.2 TOE Architecture

The TOE can control access to objects called forms and folders. Forms are used to define business process information in objects. Folders are collections of forms that represent logical constructs of business process model maps and diagrams. Combinations of forms and folders represent business processes (procedures) that the TOE can provide users interfaces with in order to view and manage.

The TOE has the ability to restrict access to forms and folders to authorized users. Users have to be assigned to a role, and Access Control Lists (ACLs) containing user and/or role identifiers are used to make access control decisions for a given object.

Non-administrative users access the TOE using a web browser in the IT environment to access the TOE HTTP network protocol interface. Users are required to provide a user name and password before a session with the TOE can be established.

Administrative users access the TOE using e-Work Engine administrator console component Windows application graphical user interface (GUI) interfaces. Administrators are required to provide a user name and password before a session with the TOE can be established.

The TOE in its intended environment can be described in terms of the following components:

- e-Work Web Extensions.ISAPI (web server plug-in) subsystem –Internet Server API (ISAPI) server library for Microsoft Internet Information Services web server that handles end user HTTP requests to e-Work Engine component, supports processing of e-Work data using web browsers.
- e-Work Engine subsystem – Server application that evaluates and processes e-Work transaction requests from end users. Processes Business Process Management (BPM) logic defined by administrators and used by end users to perform work flow management functions.
- e-Work Engine administrator console subsystem – Provides graphical user interface (GUI) Windows application interfaces to manage the e-Work Engine component. Includes the following subcomponents:
    - System Administrator application– Provides interfaces to start/stop e-Work Engine component, to configure authentication mechanisms. Accessed using Windows Microsoft Management Console (MMC) interfaces.
    - e-Work Designer application– Provides interfaces to create and modify existing procedures and their components (forms, folders). Accessed using Windows application interfaces.

  - Services Manager application– Provides interfaces to manage existing procedures (e.g. making a procedure available to users) and their components (forms, folders). Accessed using Windows Microsoft Management Console (MMC) interfaces.
  - Users and Roles application– Provides interfaces to manage users and user attributes. Accessed using Windows application interfaces.
  - Administrator Forms application– Provides interfaces to manage user session timeout.
- Operating system – Provides runtime environment for e-Work Engine component and e-Work Engine administrator console component (as well as database, web server, and web browser components).
- Database – Stores e-Work Engine component and e-Work Engine administrator console component configuration data.
- Web server – Provides runtime environment for e-Work Web Extensions.ISAPI component.
- Web browser – Provides web-based client interface to access e-Work Engine component services using the e-Work Web Extensions.ISAPI component.

2.2.1 Physical Boundaries

The components that make up the TOE are:

- e-Work Web Extensions.ISAPI subsystem
- e-Work Engine subsystem
- e-Work Engine administrator console subsystem
  - System Administrator.
  - e-Work Designer application.
  - Services Manager application
  - Users and Roles application
  - Administrator Forms application

The TOE depends on the following:

- Operating system – Windows 2000 Professional SP4 , Windows 2000 Server/Advanced Server SP4 , Windows XP Professional SP1a/SP2 , Windows Server 2003 Standard , Windows Server 2003 SP1
- Database – Microsoft SQL Server 7 (SP4) , Microsoft SQL Server 2000 (SP3a) , Oracle 9 R2 , Oracle 10G databases
- Web server – Microsoft IIS 5 SP4 running on Windows 2000 (SP4), Microsoft IIS 5.1 SP1/SP1A running on Windows XP Professional (SP1/SP1A), Microsoft IIS 6 running on Windows Server 2003 Standard
- Web browser – Netscape 4.75, IE 5.01 SP4, IE 6 SP1, IE 6 SP2

The TOE in its intended environment is depicted in the figure below.

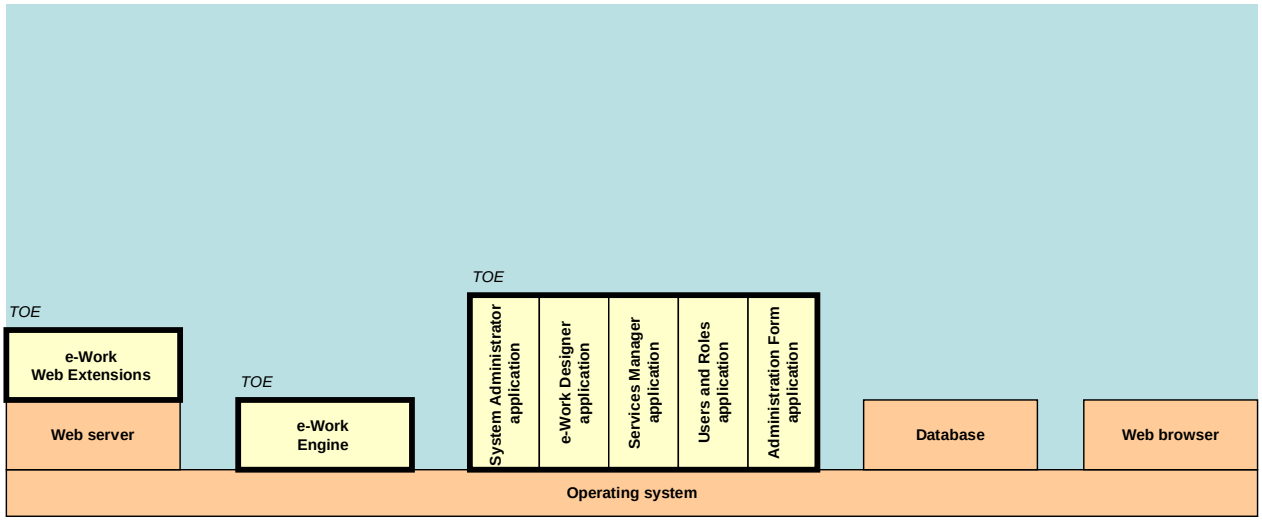

Figure 1: TOE boundary

2.2.2 Logical Boundaries

The TSF provides the following security functions:

- user data protection,
- identification and authentication,
- security management,
- protection of the TSF, and
- TOE access.

2.2.2.1 User data protection

The TOE can control access to objects called forms and folders using ACLs.

See the corresponding section in the TSS for more detailed information.

2.2.2.2 Identification and authentication

The TOE defines users in terms of security attributes that include user name, password, and role. The IT environment is relied on to authenticate administrators. The TOE offers no TSF-mediated functions until the user is identified and authenticated.

See the corresponding section in the TSS for more detailed information.

2.2.2.3 Security management

The TOE provides an administrator console that can be used to manage the TSF. The TOE maintains both administrator and user roles.

See the corresponding section in the TSS for more detailed information.

2.2.2.4 Protection of the TSF

The TOE restricts access to both its administrative and non-administrative interfaces.

See the corresponding section in the TSS for more detailed information.

2.2.2.5 TOE access

The TOE can terminate inactive interactive user sessions. The TOE relies on a timestamp provided by the operating system in the IT environment in order to determine if a session has become inactive.

See the corresponding section in the TSS for more detailed information.

2.3 TOE Documentation

Refer to Section 6 for information about the documents associated with the TOE.

3. Security Environment

The TOE security environment describes the security aspects of the intended environment in which the TOE is to be used and the manner in which it is expected to be employed. The statement of the TOE security environment defines the following:

- Threats that the TOE is designed to counter
- Assumptions made on the operational environment and the method of use intended for the TOE
- Organizational security policies to which the TOE is designed to comply

3.1 Organizational Policies

P. AUTHORIZED_USERS	Access controls will ensure that only those users who have been authorized to access the protected information within the TOE will be able to do so
P. I_AND_A	All users must be identified and authenticated prior to accessing any controlled resources
P. NEED_TO_KNOW	The TOE must limit the access to information in protected resources to those authorized users who have a need to know that information
P. ROLES	The TOE shall provide an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users

3.2 Threats

T. ADMIN_ERROR	An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms
T. MASQUERADE	An unauthorized user, process, or external IT entity may masquerade as an authorized entity to gain access to data or TOE resources
T. TSF_COMPROMISE	A malicious user or process may cause configuration data to be inappropriately accessed (viewed, modified or deleted)..
T. UNAUTH_ACCESS	A user may gain unauthorized access (view, modify, delete) to user data

3.3 Assumptions

A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.NO_EVIL	The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation.

4. Security Objectives

This section defines the security objectives of the TOE and its supporting environment. Security objectives, categorized as either IT security objectives or non-IT security objectives, reflect the stated intent to address the assumptions, counter identified threats and/or comply with any organizational security policies identified. All of the identified assumptions, threats and organizational policies are addressed under one of the categories below.

4.1 Security Objectives for the TOE

O.ACCESS	The TOE will ensure that users gain only authorized access to it and to the resources that it controls
O.ADMIN_ROLE	The TOE will provide authorized administrator roles to isolate administrative actions
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the authorized administrators in their management of the security of the TOE
O.TOE_PROTECTION	The TOE will protect itself and its assets from external interference or tampering
O.USER_AUTHENTICATION	The TOE will verify the claimed identity of users
O.USER_IDENTIFICATION	The TOE will uniquely identify users

4.2 Security Objectives for the IT Environment

OE.USER_AUTHENTICATION	The IT Environment will verify the claimed identity of administrators.
OE.USER_IDENTIFICATION	The IT Environment will uniquely identify users.

4.3 Security Objectives for the Environment

OE.CONFIG	The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation.
OE.PHYCAL	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

5. IT Security Requirements

This section defines the security functional requirements for the TOE as well as the security assurance requirements against which the TOE has been evaluated. All of the requirements have been copied from version 2.2 of the applicable Common Criteria documents.

5.1 TOE Security Functional Requirements

The following table describes the SFRs that are candidates to be satisfied by TOE.

Requirement Class	Requirement Component
FDP: User data protection	FDP_ACC.2: Complete access control
	FDP_ACF.1: Security attribute based access control
FIA: Identification and authentication	FIA_ATD.1a: User attribute definition
	FIA_UAU.2a: User authentication before any action
	FIA_UID.2: User identification before any action
FMT: Security management	FMT_MSA.1a: Management of security attributes
	FMT_MSA.1b: Management of security attributes
	FMT_MSA.3: Static attribute initialization
	FMT_MTD.1a: Management of TSF data
	FMT_MTD.1b: Management of TSF data
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_RVM.1: Non-bypassability of the TSP
FTA: TOE access	FTA_SSL.3: TSF-initiated termination

Table 1 TOE Security Functional Components

5.1.1 User data protection (FDP)

5.1.1.1 Complete access control (FDP_ACC.2)

FDP_ACC.2.1 The TSF shall enforce the **[Work Flow Access Control Policy]** on **[subjects: users; objects: forms, folders]** and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

5.1.1.2 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the **[Work Flow Access Control Policy]** to objects based on the following: **[subject security attributes: user identifier and role; object security attributes: object owner, and access control list (ACL)]**.

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) if the user identity is equal to the object owner, the requested access is allowed; or (b) if the ACL grants the requesting user identity the requested access, the requested access is allowed; (c) if the user identity is a member of a role defined for the object and the ACL grants the role the requested access, the requested access is allowed].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[(a)if the subject has the administrator role, the requested access is allowed, (b)if there is no ACL configured for a given object, the requested access is allowed]**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the **[no additional explicit deny rules]**.

5.1.2 Identification and authentication (FIA)

5.1.2.1 User attribute definition (FIA_ATD.1a)

FIA_ATD.1a.1 The TSF shall maintain the following list of security attributes belonging to individual users: **[user identity, authentication data, and role]**.

5.1.2.2 User authentication before any action (FIA_UAU.2a)

FIA_UAU.2a.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.2.3 User identification before any action (FIA_UID.2)

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.3 Security management (FMT)

5.1.3.1 Management of security attributes (FMT_MSA.1a)

FMT_MSA.1a.1 The TSF shall enforce the **[Work Flow Access Control Policy]** to restrict the ability to **[*modify*]** the security attributes **[subject security attributes: user identity, authentication data, and role]** to **[authorized administrators]**.

5.1.3.2 Management of security attributes (FMT_MSA.1b)

FMT_MSA.1b.1 The TSF shall enforce the **[Work Flow Access Control Policy]** to restrict the ability to **[*modify*]** the security attributes **[object security attributes: ACL]** to **[authorized administrators and object owners]**.

5.1.3.3 Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the **[Work Flow Access Control Policy]** 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 administrator]** to specify alternative initial values to override the default values when an object or information is created.

5.1.3.4 Management of TSF data (FMT_MTD.1a)

FMT_MTD.1a.1 The TSF shall restrict the ability to **[*modify, delete, [create]*]** the **[user accounts]** to **[authorized administrators]**.

5.1.3.5 Management of TSF data (FMT_MTD.1b)

FMT_MTD.1b.1 The TSF shall restrict the ability to **[*modify*]** the **[interactive session timeout values]** to **[authorized administrators]**.

5.1.3.6 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: **[Management of Work Flow Access Control Policy, Management of user accounts, Management of interactive session timeout value]**.

5.1.3.7 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles **[Administrator, User]**.
FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.4 Protection of the TSF (FPT)

5.1.4.1 Non-bypassability of the TSP (FPT_RVM.1)

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.5 TOE access (FTA)

5.1.5.1 TSF-initiated termination (FTA_SSL.3)

FTA_SSL.3.1 The TSF shall terminate an interactive session after a **[administrator configurable amount of time]**.

5.2 IT Environment Security Functional Requirements

The following table describes the SFRs that are candidates to be satisfied by the IT environment of the TOE.

Requirement Class	Requirement Component
FIA: Identification and authentication	FIA_ATD.1b: User attribute definition
	FIA_UAU.2b: User authentication before any action
FPT: Protection of the TSF	FPT_STM.1: Reliable time stamps

Table 2 IT Environment Security Functional Components

5.2.1 Identification and authentication (FIA)

5.2.1.1 User attribute definition (FIA_ATD.1b)

FIA_ATD.1b.1 The ~~TSF~~ **IT Environment** shall maintain the following list of security attributes belonging to individual users: **[user identity and authentication data]**.

5.2.1.2 User authentication before any action (FIA_UAU.2b)

FIA_UAU.2b.1 The ~~TSF~~ **IT Environment** shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.2.2 Protection of the TSF (FPT)

5.2.2.1 Reliable time stamps (FPT_STM.1)

FPT_STM.1.1 The ~~TSF~~ **IT Environment** shall be able to provide reliable time stamps for its own use.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ACM: Configuration management	ACM_CAP.2: Configuration items
ADO: Delivery and operation	ADO_DEL.1: Delivery procedures
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1: Informal functional specification
	ADV_HLD.1: Descriptive high-level design
	ADV_RCR.1: Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.1: Developer vulnerability analysis

Table 3 EAL 2 Assurance Components

5.3.1 Configuration management (ACM)

5.3.1.1 Configuration items (ACM_CAP.2)

ACM_CAP.2.1d The developer shall provide a reference for the TOE.
ACM_CAP.2.2d The developer shall use a CM system.
ACM_CAP.2.3d The developer shall provide CM documentation.
ACM_CAP.2.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.2.2c The TOE shall be labelled with its reference.
ACM_CAP.2.3c The CM documentation shall include a configuration list.
ACM_CAP.2.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.2.5c The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.2.6c The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.2.7c The CM system shall uniquely identify all configuration items.
ACM_CAP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and operation (ADO)

5.3.2.1 Delivery procedures (ADO_DEL.1)

ADO_DEL.1.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2d The developer shall use the delivery procedures.
ADO_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.
ADO_DEL.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1d The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1c The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.

ADO_IGS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2e The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development (ADV)

5.3.3.1 Informal functional specification (ADV_FSP.1)

ADV_FSP.1.1d The developer shall provide a functional specification.

ADV_FSP.1.1c The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2c The functional specification shall be internally consistent.

ADV_FSP.1.3c The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4c The functional specification shall completely represent the TSF.

ADV_FSP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.2 Descriptive high-level design (ADV_HLD.1)

ADV_HLD.1.1d The developer shall provide the high-level design of the TSF.

ADV_HLD.1.1c The presentation of the high-level design shall be informal.

ADV_HLD.1.2c The high-level design shall be internally consistent.

ADV_HLD.1.3c The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5c The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6c The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2e The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1d The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1c For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

ADV_RCR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Guidance documents (AGD)

5.3.4.1 Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1d The developer shall provide administrator guidance addressed to system administrative personnel.
AGD_ADM.1.1c The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.
AGD_ADM.1.2c The administrator guidance shall describe how to administer the TOE in a secure manner.
AGD_ADM.1.3c The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.
AGD_ADM.1.4c The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.
AGD_ADM.1.5c The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.
AGD_ADM.1.6c The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_ADM.1.7c The administrator guidance shall be consistent with all other documentation supplied for evaluation.
AGD_ADM.1.8c The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.
AGD_ADM.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1d The developer shall provide user guidance.
AGD_USR.1.1c The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.
AGD_USR.1.2c The user guidance shall describe the use of user-accessible security functions provided by the TOE.
AGD_USR.1.3c The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
AGD_USR.1.4c The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.
AGD_USR.1.5c The user guidance shall be consistent with all other documentation supplied for evaluation.
AGD_USR.1.6c The user guidance shall describe all security requirements for the IT environment that are relevant to the user.
AGD_USR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5 Tests (ATE)

5.3.5.1 Evidence of coverage (ATE_COV.1)

ATE_COV.1.1d The developer shall provide evidence of the test coverage.
ATE_COV.1.1c The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_COV.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.2 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.
ATE_FUN.1.2d The developer shall provide test documentation.

ATE_FUN.1.1c The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2c The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.3c The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4c The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5c The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.
ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5.3 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.
ATE_IND.2.1c The TOE shall be suitable for testing.
ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2e The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.
ATE_IND.2.3e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.6 Vulnerability assessment (AVA)

5.3.6.1 Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1d The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.
AVA_SOF.1.1c For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.
AVA_SOF.1.2c For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.
AVA_SOF.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_SOF.1.2e The evaluator shall confirm that the strength claims are correct.

5.3.6.2 Developer vulnerability analysis (AVA_VLA.1)

AVA_VLA.1.1d The developer shall perform a vulnerability analysis.
AVA_VLA.1.2d The developer shall provide vulnerability analysis documentation.
AVA_VLA.1.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.
AVA_VLA.1.2c The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.
AVA_VLA.1.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.
AVA_VLA.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VLA.1.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

6.1.1 User data protection

The TOE implements a Work Flow Access Control Policy for object access based on:

- user identities,
- object ownership,
- assigned roles, and
- Access Control Lists (ACLs).

The TOE objects subject to this policy are forms and folders. Forms are used to define business process information in objects. Folders are collections of forms that represent logical constructs of business process model maps and diagrams. Combinations of forms and folders represent business processes (procedures) that the TOE can provide users interfaces with in order to view and manage. For example, an airline could model ticket sales in a map as follows:

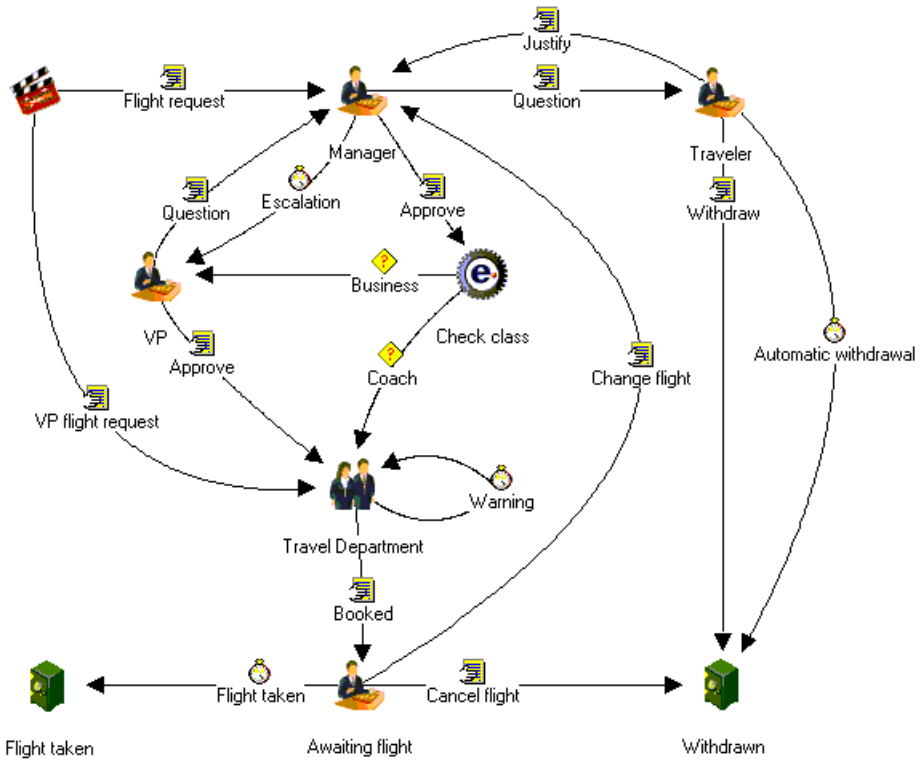

Figure 2: Sample business process model map

The above map depicts the following possible business process work flows:

- An employee may be asked to justify their travel request.

- An employee may cancel or withdraw their travel request, ending the procedure.
- A request for a business-class flight is directed to a manager (VP in the above diagram stands for Vice President, simply intended as an identifier in the example, not intended to identify an additional VP role supported by the TOE) for second approval , while a request for a coach flight goes directly to the travel department after initial approval.
- Travel plans may be changed or cancelled, ending the procedure before the scheduled flight date.
- A request may be approved, travel scheduled, and the flight taken, ending the procedure.

The TOE has the ability to restrict access to forms and folders to their owners and to administrators. Users may be assigned to an ACL; ACLs containing user identifiers are used to make access control decisions for a given object. Similarly, users may be assigned to a role, and ACLs containing user and/or role identifiers are used to make access control decisions for a given object.

Roles are a way of grouping users in an organization. A user can have any number of roles, and a role can be assigned to one or many users. Roles are created during the procedure design process and added to the e-Work database when a procedure is published. The procedure design process consists of creating maps (folders) and forms in order to build business rules that are used to automate business processes.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_ACC.2, FDP_ACF.1: All users are subject to the Work Flow Access Control Policy for all available operations on forms and folders.

6.1.2 Identification and authentication

The TOE defines users in terms of:

- user identity,
- authentication data, and
- roles.

The TOE provides its own username and password authentication mechanism that it uses to authenticate non-administrative users. While the product supports additional authentication mechanisms, only username/password in general is supported in the evaluated configuration. In order to access the TOE, a user account including a user name and password must be created for the user.

Non-administrative users access the TOE using a web browser in the IT environment to access the TOE HTTP network protocol interface. Users are required to provide a user name and password before a session with the TOE can be established.

Administrative users access the TOE using e-Work Engine administrator console component Windows application graphical user interface (GUI) interfaces. Administrators are required to provide a user name and password before a session with the TOE can be established. The administrator user name and password are then forwarded to the database in the IT environment for authentication.

Note that the TOE does not implement any password composition rules or minimum password lengths. Administrative guidance is relied on to ensure that when user accounts are created, a minimum password length of eight printable characters is used.

The Identification and authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1a: The TOE defines users in terms of security attributes that include user name, password, and role.
- FIA_UAU.2a: The TOE offers no TSF-mediated functions until the user is authenticated. The TOE authenticates non-administrative users using its username/password mechanism. The TOE relies on the database in the IT environment to authenticate administrators.
- FIA_UID.2: The TOE offers no TSF-mediated functions until the user is identified.

6.1.3 Security management

The TOE provides administrators with Windows application graphical user interface (GUI) interfaces to create and manage process flows, and to manage the security functions of the TOE. An administrator console can be logically described as the e-Work Engine administrator console component. The e-Work Engine administrator console component includes the following Windows applications:

- System Administrator application
- Services Manager application
- e-Work Designer application
- Users and Roles application
- Administration Form application

The e-Work Engine administrator console component interfaces include those that can perform the following management functions:

- management of subjects and authentication data
- management of objects
- management of session inactivity settings

Administrator console interfaces can only be called by administrators, with the exception of interfaces to manage objects, which can be called by object owners to modify owned object ACLs. Users that have been assigned the administrator role are considered authorized administrators, all others are simply users.

The Security management function is designed to satisfy the following security functional requirements:

- FMT_MSA.1a: The ability to manage subject attributes that are maintained by the TOE is restricted to an administrator by restricting access to administrative console interfaces.
- FMT_MSA.1b: The ability to manage object attributes is restricted to an administrator or object owner by restricting access to administrative console interfaces.
- FMT_MSA.3: By default every object is created with the creator as the owner. Subsequently, access can be granted to other users. The administrator can specify alternative values.
- FMT_MTD.1a: This requirement is met because the TOE restricts the ability to modify, delete, and create user accounts to authorized administrators by restricting access to administrative console interfaces.
- FMT_MTD.1b: This requirement is met because the TOE restricts the ability to modify the settings for an interactive session to authorized administrators by restricting access to administrative console interfaces.
- FMT_SMF.1: The TOE provided administrator console interfaces to manage the Work Flow Access Control Policy, to manage user accounts, and to manage inactive session threshold values.
- FMT_SMR.1: Users that have been assigned the administrator role are considered authorized administrators, all others are simply users.

6.1.4 Protection of the TSF

When a user, without the necessary role, requests communication with the TOE access is denied. Users cannot proceed to use their TOE role until they have supplied a user name and password that corresponds to the TOE access list.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_RVM.1: The TOE security functions are invoked and succeed before each function within the TSC is allowed to proceed.

6.1.5 TOE access

TOE Administrators set the session time-out period for users accessing the TOE. The default for this setting is 60 minutes.

The TOE access function is designed to satisfy the following security functional requirements:

- FTA_SSL.3: The TOE can terminate a user's interactive session after an administrator set time period that must be greater than zero.

6.2 TOE Security Assurance Measures

The following assurance measures are applied to satisfy the Common Criteria EAL 2 assurance requirements:

- Configuration Management;
- Delivery and Guidance;
- Design Documentation;
- Lifecycle Support;
- Tests; and
- Vulnerability Assessment.

6.2.1 Configuration management

The configuration management measures applied by Metastorm ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. Metastorm performs configuration management on the TOE implementation representation, design, tests, user and administrator guidance, and the CM documentation.

These activities are documented in:

- Metastorm Configuration Management Plan April 2005, Metastorm e-Work Product Lifecycle, 2004

The Configuration management assurance measure satisfies the following EAL 2 assurance requirements:

- ACM_CAP.2

6.2.2 Delivery and operation

Metastorm provides delivery documentation and procedures to identify the TOE, secure the TOE during delivery, and provide necessary installation and generation instructions. Metastorm's delivery procedures describe all applicable procedures to be used to prevent in appropriate access to the TOE. Metastorm also provides documentation that describes the steps necessary to install Metastorm e-Work in accordance with the evaluated configuration.

These activities are documented in:

- Metastorm Delivery Plan April 2005

The Delivery and operation assurance measure satisfies the following EAL 2 assurance requirements:

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Development

Metastorm has documents describing all facets of the design of the TOE. These documents serve to describe the security functions of the TOE, its interfaces both external and between subsystems, the architecture of the TOE (in terms of subsystems), and correspondence between the available design abstractions (including the ST).

These activities are documented in:

- Metastorm High Level Design April 2005 and Metastorm Functional Specification April 2005

The Development assurance measure satisfies the following EAL 2 assurance requirements:

- ADV_FSP.1
- ADV_HLD.1
- ADV_RCR.1

6.2.4 Guidance documents

Metastorm provides administrator and user guidance on how to utilize the TOE security functions and warnings to administrators and users about actions that can compromise the security of the TOE.

These activities are documented in:

- Metastorm eWork Release 6.6 Administration Guide, July 2004; Metastorm eWork Release 6.6 Designer User Manual; July 2004, Metastorm eWork Release 6.6 Web Authors Guide, July 2004; Metastorm eWork Release 6.6 Deployment Guide, July 2004; Metastorm eWork Release 6.6 Release Notes, September 2004; Metastorm e-Work Directions, 2005; Metastorm eWork™ Release 6.6 e-Work Concepts, July 2004; Metastorm eWork Release 6.6 e-Work Installation Prerequisites, July 2004; Metastorm eWork Release 6.6 Installation Guide, July 2004

The Guidance documents assurance measure satisfies the following EAL 2 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Tests

The test documents describe the overall test plan, testing procedures, the tests themselves, including expected and actual results. In addition, these documents describe how the functional specification has been appropriately tested.

These activities are documented in:

- Metastorm Test Plan April 2005

The Tests assurance measure satisfies the following EAL 2 assurance requirements:

- ATE_COV.1
- ATE_FUN.1
- ATE_IND.2

6.2.6 Vulnerability assessment

Metastorm has conducted a strength of function analysis wherein all permutation or probabilistic security mechanisms have been identified and analyzed resulting in a demonstration that all of the relevant mechanisms fulfill the minimum strength of function claim, SOF-basic.

Metastorm performs regular vulnerability analyses of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE.

These activities are documented in:

- Metastorm eWork Release 6.6 Release Notes, September 2004; Metastorm Vulnerability Assessment Release Notes

The Vulnerability assessment assurance measure satisfies the following EAL 2 assurance requirements:

- AVA_SOF.1
- AVA_VLA.1

7. Protection Profile Claims

There is no Protection Profile claim in this Security Target.

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Strength of Functions;
- Requirement Dependencies;
- TOE Summary Specification; and,
- PP Claims.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of organizational policies and usage assumptions by the security objectives.

	O.ACCESS	O.ADMIN_ROLE	O.MANAGE	O.TOE_PROTECTION	O.USER_AUTHENTICATION	O.USER_IDENTIFICATION	OE.USER_IAUTHENTICATION	OE.USER_IDENTIFICATION	OE.CONFIG	OE.PHYCAL
P.AUTHORIZED_USERS	x									
P.I_AND_A					x	x	x	x		
P.NEED_TO_KNOW	x					x		x		
P.ROLES		x								
T.ADMIN_ERROR			x							
T.MASQUERADE					x		x			
T.TSF_COMPROMISE				x						
T.UNAUTH_ACCESS	x	x								
A.LOCATE										x
A.NO_EVIL									x	

Table 4 Environment to Objective Correspondence

8.1.1.1 P. AUTHORIZED_USERS

Access controls will ensure that only those users who have been authorized to access the protected information within the TOE will be able to do so.

This Organizational Policy is satisfied by ensuring that:

- O.ACCESS: The TOE will ensure that users gain only authorized access to it and to the resources that it controls.

8.1.1.2 P. I_AND_A

All users must be identified and authenticated prior to accessing any controlled resources.

This Organizational Policy is satisfied by ensuring that:

- O.USER_AUTHENTICATION: The TOE will verify the claimed identity of users.
- O.USER_IDENTIFICATION: The TOE will uniquely identify users.
- OE.USER_AUTHENTICATION: The TOE relies on the database in the IT environment to authenticate administrators.
- OE.USER_IDENTIFICATION: The IT environment is relied on to maintain user name and authentication data for a given user identity.

8.1.1.3 P. NEED_TO_KNOW

The TOE must limit the access to information in protected resources to those authorized users who have a need to know that information.

This Organizational Policy is satisfied by ensuring that:

- O.ACCESS: The TOE will ensure that users gain only authorized access to it and to the resources that it controls.
- O.USER_IDENTIFICATION: The TOE will uniquely identify users.
- OE.USER_IDENTIFICATION: The IT environment is relied on to maintain user name and authentication data for a given user identity.

8.1.1.4 P. ROLES

The TOE shall provide an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.

This Organizational Policy is satisfied by ensuring that:

- O.ADMIN_ROLE: The TOE will provide authorized administrator roles to isolate administrative actions.

8.1.1.5 T. ADMIN_ERROR

An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.

This Organizational Policy is satisfied by ensuring that:

- O.MANAGE: The TOE will provide all the functions and facilities necessary to support the authorized administrators in their management of the security of the TOE.

8.1.1.6 T. MASQUERADE

An unauthorized user, process, or external IT entity may masquerade as an authorized entity to gain access to data or TOE resources.

This Threat is countered by ensuring that:

- O.USER_AUTHENTICATION: The TOE will verify the claimed identity of users.
- OE.USER_AUTHENTICATION: The TOE relies on the database in the IT environment to authenticate administrators.

8.1.1.7 T. TSF_COMPROMISE

A malicious user or process may cause configuration data to be inappropriately accessed (viewed, modified or deleted)..

This Threat is countered by ensuring that:

- O.TOE_PROTECTION: The TOE will protect itself and its assets from external interference or tampering.

8.1.1.8 T. UNAUTH_ACCESS

A user may gain unauthorized access (view, modify, delete) to user data.

This Threat is countered by ensuring that:

- O.ACCESS: The TOE will ensure that users gain only authorized access to it and to the resources that it controls.
- O.ADMIN_ROLE: The TOE will provide authorized administrator roles to isolate administrative actions.

8.1.1.9 A. LOCATE

The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

This Assumption is satisfied by ensuring that:

- OE.PHYCAL: The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

8.1.1.10 A. NO_EVIL

The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation.

This Assumption is satisfied by ensuring that:

- OE.CONFIG: The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that **Table 5** indicates the requirements that effectively satisfy the individual objectives. .

8.2.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

	O.ACCESS	O.ADMIN_ROLE	O.MANAGE	O.TOE_PROTECTION	O.USER_AUTHENTICATION	O.USER_IDENTIFICATION	OE.USER_AUTHENTICATION	OE.USER_IDENTIFICATION
FDP_ACC.2	x							
FDP_ACF.1	x							
FIA_ATD.1a						x		
FIA_ATD.1b								x
FIA_UAU.2a					x			
FIA_UAU.2b							x	
FIA_UID.2						x		
FMT_MSA.1a			x					
FMT_MSA.1b			x					
FMT_MSA.3			x					
FMT_MTD.1a			x					
FMT_MTD.1b			x					
FMT_SMF.1			x					
FMT_SMR.1		x	x					
FPT_RVM.1				x				
FTA_SSL.3	x							
FPT_STM.1	x							

Table 5 Objective to Requirement Correspondence

8.2.1.1 O.ACCESS

The TOE will ensure that users gain only authorized access to it and to the resources that it controls

This TOE Security Objective is satisfied by ensuring that:

- FDP_ACC.2, FDP_ACF.1: All users are subject to the Work Flow Access Control Policy for all available operations on forms and folders.
- FTA_SSL.3: This requirement is met because the TOE terminates a user's interactive session after an administrator set time period that must be greater than zero.
- FPT_STM.1: The TOE relies on a timestamp provided by the operating system in the IT environment in order to determine if a session has become inactive.

8.2.1.2 O.ADMIN_ROLE

The TOE will provide authorized administrator roles to isolate administrative actions.

This TOE Security Objective is satisfied by ensuring that:

- FMT_SMR.1: Users that have been assigned the administrator role are considered authorized administrators, all others are simply users.

8.2.1.3 O.MANAGE

The TOE will provide all the functions and facilities necessary to support the authorized administrators in their management of the security of the TOE.

This TOE Security Objective is satisfied by ensuring that:

- FMT_MSA.1a: The ability to manage subject attributes that are maintained by the TOE is restricted to an administrator by restricting access to administrative console interfaces.
- FMT_MSA.1b: The ability to manage object attributes is restricted to an administrator by restricting access to administrative console interfaces.
- FMT_MSA.3: By default every object is created with the creator as the owner. Subsequently, access can be granted to other users. The administrator can specify alternative values.
- FMT_MTD.1a: This requirement is met because the TOE restricts the ability to modify, delete, and create user accounts to authorized administrators by restricting access to administrative console interfaces.
- FMT_MTD.1b: This requirement is met because the TOE restricts the ability to modify the settings for an interactive session to authorized administrators by restricting access to administrative console interfaces.
- FMT_SMF.1: The TOE provided administrator console interfaces to manage the Work Flow Access Control Policy, to manage user accounts, and to manage inactive session threshold values.
- FMT_SMR.1: Users that have been assigned the administrator role are considered authorized administrators, all others are simply users.

8.2.1.4 O.TOE_PROTECTION

The TOE will protect itself and its assets from external interference or tampering.

This TOE Security Objective is satisfied by ensuring that:

- FPT_RVM.1: The TOE security functions are invoked and succeed before each function within the TSC is allowed to proceed.

8.2.1.5 O.USER_AUTHENTICATION

The TOE will verify the claimed identity of users.

This TOE Security Objective is satisfied by ensuring that:

- FIA_UAU.2a: The TOE offers no TSF-mediated functions until the user is authenticated. The TOE authenticates non-administrative users using its username/password mechanism.

8.2.1.6 O.USER_IDENTIFICATION

The TOE will uniquely identify users.

This TOE Security Objective is satisfied by ensuring that:

- FIA_ATD.1a: The TOE defines users in terms of security attributes that include user name, password, and role.
- FIA_UID.2: The TOE offers no TSF-mediated functions until the user is identified.

8.2.1.7 OE.USER_ AUTHENTICATION

The IT Environment will verify the claimed identity of administrators.

This IT Environment Security Objective is satisfied by ensuring that:

- FIA_UAU.2b: The TOE relies on the database in the IT environment to authenticate administrators.

8.2.1.8 OE.USER_IDENTIFICATION

The IT Environment will uniquely identify users.

This IT Environment Security Objective is satisfied by ensuring that:

- FIA_ATD.1b: The IT environment defines users in terms of security attributes that include user name and authentication data for a given user identity.

8.3 Security Assurance Requirements Rationale

EAL2 was selected as the assurance level because the TOE is a commercial product whose users require a low to moderate level of independently assured security. Metastorm e-Work is targeted at a relatively benign environment with good physical access security and competent administrators. Within such environments it is assumed that attackers will have little attack potential. As such, EAL2 is appropriate to provide the assurance necessary to counter the limited potential for attack.

8.4 Strength of Functions Rationale

The overall strength of function claim of SOF-basic is believed to be commensurate with the overall assurance claim of EAL 2. The only applicable security function is Identification and Authentication where passwords are used by users as evidence of their claimed identities. The intent is that the password mechanism meets or exceeds SOF-basic and the evidence can be found in the strength of function analysis included in Metastorm e-Work Vulnerability Analysis.

8.5 Requirement Dependency Rationale

The following table demonstrates that all dependencies among the claimed security requirements are satisfied and therefore the requirements work together to accomplish the overall objectives defined for the TOE.

ST Requirement	CC Dependencies	ST Dependencies
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.2 and FMT_MSA.3
FIA_ATD.1	none	none
FIA_UAU.2a	FIA_UID.1	FIA_UID.2
FIA_UAU.2b	FIA_UID.1	FIA_UID.2
FIA_UID.2	none	none
FMT_MSA.1a	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_ACC.2
FMT_MSA.1b	FMT_SMR.1 and FMT_SMF.1 and (FDP_ACC.1 or FDP_IFC.1)	FMT_SMR.1 and FMT_SMF.1 and FDP_ACC.2
FMT_MSA.3	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1 and FMT_SMR.1
FMT_MTD.1a	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MTD.1b	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_SMF.1	none	none
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_RVM.1	none	none
FTA_SSL.3	none	none

FPT_STM.1	none	none
ACM_CAP.2	none	none
ADO_DEL.1	none	none
ADO_IGS.1	AGD_ADM.1	AGD_ADM.1
ADV_FSP.1	ADV_RCR.1	ADV_RCR.1
ADV_HLD.1	ADV_FSP.1 and ADV_RCR.1	ADV_FSP.1 and ADV_RCR.1
ADV_RCR.1	none	none
AGD_ADM.1	ADV_FSP.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1	ADV_FSP.1
ATE_COV.1	ADV_FSP.1 and ATE_FUN.1	ADV_FSP.1 and ATE_FUN.1
ATE_FUN.1	none	none
ATE_IND.2	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1
AVA_SOF.1	ADV_FSP.1 and ADV_HLD.1	ADV_FSP.1 and ADV_HLD.1
AVA_VLA.1	ADV_FSP.1 and ADV_HLD.1 and AGD_ADM.1 and AGD_USR.1	ADV_FSP.1 and ADV_HLD.1 and AGD_ADM.1 and AGD_USR.1

8.6 Explicitly Stated Requirements Rationale

There are no explicitly stated requirements in this Security Target.

8.7 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 6 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	User data protection	**Identification and authentication**	**Security management**	**Protection of the TSF**	**TOE access**
FDP_ACC.2	X				
FDP_ACF.1	X				
FIA_ATD.1a		X			
FIA_UAU.2a		X			
FIA_UID.2		X			
FMT_MSA.1a			X		
FMT_MSA.1b			X		
FMT_MSA.3			X		
FMT_MTD.1a			X		
FMT_MTD.1b			X		

FMT_SMF.1			X		
FMT_SMR.1			X		
FPT_RVM.1				X	
FTA_SSL.3					X

Table 6 Security Functions vs. Requirements Mapping

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.