Secutor Systems, Inc. DataVault X4 v1.0

EAL4 Security Target

Version 1.0

23 September 2005

Prepared for:

Secutor Systems, Inc.

1228 S. Military Highway, Suite B
Chesapeake, VA 23320

Prepared By:

Science Applications International Corporation

Common Criteria Testing Laboratory

7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

LIST OF FIGURES

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 DataVault X4 provided by Secutor Systems, Inc. Systems. The purpose of the DataVault X4 is to provide a dual secure computer with multi-domain, multi-network and multi-tasking capabilities for processing classified and unclassified data within one PC.

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 and the threats that are countered by TOE and it environment.
- 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 the TOE and IT Environment that supports the TOE, and details the assurance requirements for EAL4.
- TOE Summary Specification (Section 6) - The section describes the security functions represented in the TOE that satisfy the security requirements.
- Protection Profile Claims (Section 7) - This section presents any protection profile claims.
- 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 – Secutor Systems, Inc. DataVault X4 v1.0 EAL4 Security Target

ST Version – Version 1.0

ST Date – 23 September 2005

TOE Identification – Secutor Systems, Inc. DataVault X4 v1.0

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
  - EAL 4

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, a letter placed at the end of the component indicates an iteration. 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.

1.3.2 Terminology and Acronyms

The following terminology and acronyms may be used within this Security Target.

Acronyms	
CC	Common Criteria
CAC	Common Access Card
CEM	Common Evaluation Methodology
CCEVS	Common Criteria Evaluation and Validation Scheme
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HLD	High-level Design
LAN	Local Area Network
NIC	Network Interface Card
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OS	Operating system
PCMCIA (card)	Personal Computer Memory Card International Association (card)
PP	Protection Profile
SAIC	Science Applications International Corporation
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

Terminology	
K&M Switch	Hardware Domain Selection Switch (K&M) to control one keyboard and one mouse for a specific domain.
Key #1	A physical key to the front and back panel of the TOE so that devices and network cablings can be maintained. This key is normally restricted to the Key Administrator.
Key #2	A physical key to turn on and off each DataVault X4. Each key # 2 is specific to each DataVault X4. This key is required to boot the computer to the UNSECURE domain. This key is assigned to users and trusted users. The Key Administrator also has access to this key since Key #2 is also used to deactivate or activate the “open case alarm” located inside the back panel of the TOE.
Key #3	A physical key that is used to remove a SECURE hard drive or install a SECURE hard drive (or blank drive). This key is normally restricted to trusted users. The Key Administrator may also have access to this key.
multi-domain	Two-domain configuration that consist of one UNSECURE domain and one SECURE domain. Each domain isolated where no information is shared or crossed between the domains.

2. TOE Description

The Target of Evaluation (TOE) is Secutor Systems, Inc. DataVault X4 v1.0. The purpose of the DataVault X4 is to provide a dual secure computer with multi-domain, multi-network and multi-tasking capabilities for processing classified and unclassified data within one PC. As such, the TOE provides two completely isolated security domains where no information is shared or crossed between each of the domains. The DataVault X4 provides hardware-based access control mechanisms and Smart Card access control. When describing two-domain configurations, one domain is called the UNSECURE domain and the other domain is called the SECURE domain. They share no common components with the exception of the keyboard, mouse, case with power supply, and K&M switch. All information, such as user data, applications, and operating system that resides on the hard drive in one domain is separate from the other domain. Thus, each domain could have a different operating system. This configuration assures that no data can flow from one domain to the other because each domain is totally isolated and separate from the other.

2.1 TOE Overview

The DataVault X4 is built within a single rack mounted cabinet with locked panels to restrict access to both the front and back of the TOE. The locked front panel cover restricts user access to the computer interface, and the locked back panel cover restricts unauthorized access to all port and network connections. Access to the panels requires key #1. Additionally, there is a case-open alarm that can only be disabled through a lock that is inside the back lockable cover. When enabled, the open case alarm emits a loud sound if the Top panel is compromised. When the auditable alarm sounds, the alarm will automatically stop when the Top panel is replaced.

Once the Key Administrator provides access to the TOE by unlocking the front cover, the user needs key #2 for the On/Off switch to turn on the system, which provides the user access only to the UNSECURE domain. When a trusted user or Key Administrator wishes access to the SECURE domain, the user must first double click on the keyboard mounted Internal Secure Switch (Keyboard Hotkey Control) marked as Scroll/Lock key then the arrow up or arrow down key or depresses the "domain selector switch" mounted on the front of the TOE. The trusted user or Key Administrator is then prompted to perform a mandatory access control identification and authentication process through the use of a CAC or Smart Card interface mounted on the front of the TOE. The user must enter a Smart Card into a Smart Card reader to proceed with the mandatory access control identification and authentication process. If the Smart Card reader provides a positive response from the authentication request made by the TOE back to the TOE, the trusted user or Key Administrator is granted access to the SECURE hardware-based domain and SECURE removable hard drive. A user may toggle and attempt to access the SECURE domain, though access is not granted to the user unless they possess a Smart card and can pass the Smart Card mandatory access control identification and authentication process. The exception is when the Key Administrator is an administrator of the SECURE domain operating system and the IT environment authentication server; here, the Key Administrator is required to be authenticated before access is granted, but does not require a Smart Card.

Once access to the SECURE domain is granted, the trusted user or Key Administrator may switch back and forth between the UNSECURE and SECURE domain by double clicking the keyboard hotkey "Scroll/Lock" key and then the "Arrow Up" or the "Arrow Down" key once or by depressing the domain selector switch mounted on the front of the TOE once. When the TOE switches between domains all data access via the keyboard and mouse is suspended in the domain that is being exited. The cursor on the exited monitor remains stationary and the keyboard is non-functional in the exited domain. When the exited domain is again selected, data processing continues at the point where the domain was last exited. No information flows from one domain to another before, during, or after a domain switch. The only way to transfer data and information from the UNSECURE to the SECURE domains is through the use of a floppy disk or CD/ROM by a trusted user. The Read/Write function of the floppy on the UNSECURE domain is enabled. The Write function of the Floppy Drive and DVD or CD/ROM on the SECURE domain is mechanically disabled so data cannot be copied onto a floppy disk or CD from the SECURE network or SECURE removable hard drive. This prevents data theft from the SECURE domain, even when a trusted user is accessing it. In summary, data can be transferred from the UNSECURE domain to the SECURE by a trusted user or

Key Administrator but not vice-versa. There is one exception. The Key Administrator can export data from the SECURE domain by opening the back panel with key #1 and accessing the mass storage device port.

The hard drive for the UNSECURE domain is not removable. The hard drive in the SECURE domain is removable. To remove the SECURE hard drive the trusted user or Key Administrator must have in their possession key #3. The physical key must be inserted into a lock on the chassis tray for the hard drive. If the physical key and the lock match, the trusted user may remove the SECURE hard drive and place it in a safe or securely transport it.

2.2 TOE Architecture

The purpose of the DataVault4 is to provide two completely isolated hardware-based security domains where no information, memory, storage devices, BIOS, and CPU is shared between each domain. When describing the multi-domain configuration, one domain is called the UNSECURE domain and the other domain is called the SECURE domain.

2.2.1 Physical Boundaries

Each DataVault X4 computing domain shares a mouse, keyboard and a power supply with the other domain. The DataVault X.4 has one main hardware configuration option as follows:

- One dual monitor, one mouse, one keyboard, one power supply, two completely separate security domains

Note: Even if an intelligent power supply is used that can send a signal to the computing hardware, the only information flow to the power supply from a domain is uni-directional.

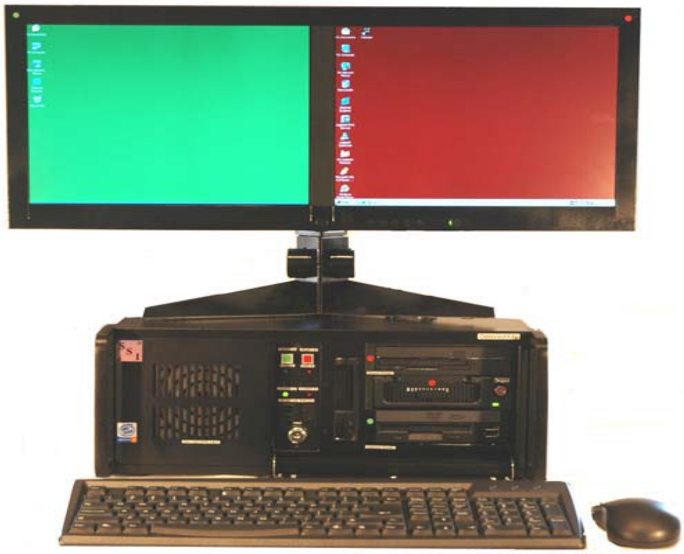

Figure 1 TOE configuration: Two security domains, each with its own monitor

The DataVault X4 workstation includes the hardware and software identified below (or their functional equivalents) as well as the user documentation provided.

- SSI case
- Domain selector switch (K&M) 2 port
- SSI power pack
- Processor: CPU - Intel Pentium IV x 2

- Motherboard: AAEON P860 x 2
- Chipset: Intel 440BX
- BIOS:
    - 2 MB AMI Flash BIOS
    - APM 1.2, DMI 2.1, Plug and Play
- Memory: 512 MB DDR 333 x 2
- Video: (64MB) Intel (build-in)
- Hard Drives:
    - 80.0GB ATA (internal)
    - 80.0GB ATA (removable. Secure domain)
- 5.5-inch removable SECURE hard drive case (1)
- CD-ROM: CD-ROM drive x 1 (slim secure domain)
- DVD/CDRW drive x 1 (slim unsecured domain)
- Floppy drive: 3.5-inch 1.44MB x 1 (slim secure domain)
- Floppy drive: 3.5-inch 1.44MB x 1 (unsecured domain)
- Network Interface Card (NIC): Intel x 2
- Keyboard: STC E05300
- Mouse or Trackball
- Monitor: dual Double Sight 15-inch LCD x 2
- Sound Card: Creative SB16
- Speakers: Mli-699
- Tamper-proof case
- Fortezza FIPS 140-1/2 certified crypto/Smart Card identification and authentication combo drive
- Operating System: Windows 2000
- Keys # 1, 2, 3 (one set)
- Cables

The DataVault X4 uses an Argus 3015 Dual Card Reader Version 1.01 that combines a FORTEZZA PCMCIA card slot for encryption and a standard ISO7816 SmartCard reader for Identification and Authentication into a single unit. The TOE only provides the hardware means for the above functions. It is the responsibility of the government agency to provide the software mechanism for identification and authentication of each user on a centralized secured network location (authentication server) as well as the FORTEZZA PCMCIA card and libraries. The encryption of the SECURE hard drive is outside the scope of the TOE and the evaluation.

To gain a perspective of the internal components of the DataVault X4, the following diagram illustrates the internal components of each domain; shared and non-shared.

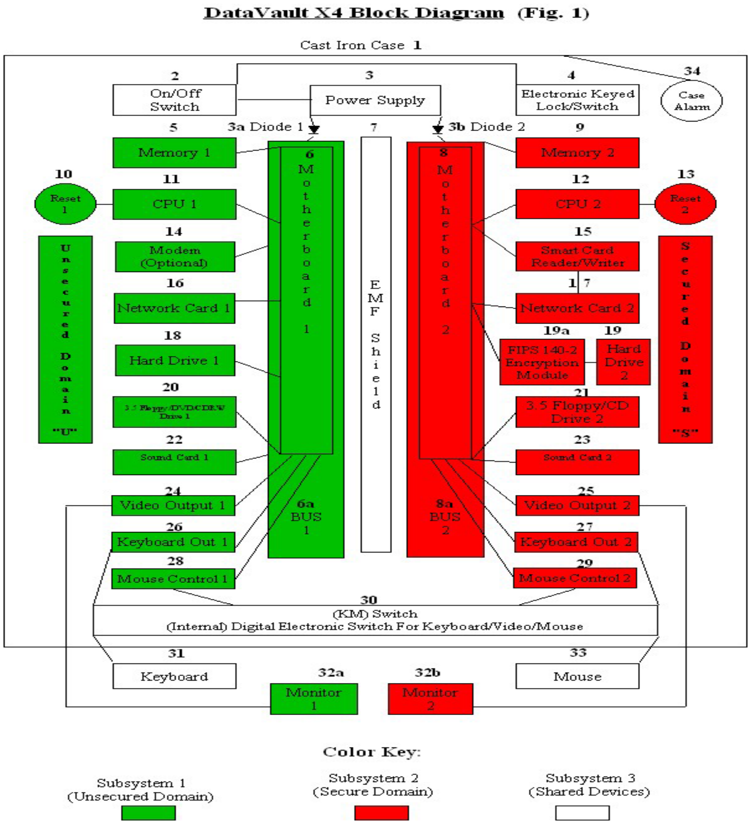

Figure 2 Internal DataVault X4 components

The TOE is intended to be used in a controlled environment with restricted access. Usually intended to be operated in facilities that users need to be identified and authenticated before entering the facility. If connected to an internal or external network, the TOE cannot be used as a gateway into another network. For instance, on the unsecured side only, a dedicated network interface card (NIC), a floppy drive, and a hard disk drive are available. On the secured side only, a different NIC and a removable hard disk drive are available; the "write" function of the SECURE domain floppy drive and CD-ROM has been disabled. Thus, in a typical case, only on the unsecured side can non-secure communication networks (e.g., internet, non-secure LAN, public telephone system) be accessed and data imported via a floppy disk drive, and only on the secured side can a secure local area network (LAN) and a secure removable hard drive be accessed. The actual classifications or types of data to be processed on the DataVault X4 are to be determined by the organization using the system.

The TOE is not expected to provide security features and controls (e.g., operating system, file access controls) necessary for a user to interact with a specific operating environment.

2.2.2 Logical Boundaries

The logical boundaries of the TOE include the security functions implemented at the TOE interfaces. These functions include user data protection, mandatory access control and identification and authentication, security management, and protection of the TSF.

2.2.2.1 User data protection

The TOE provides complete information flow control between security domains where each of the domains (SECURE and UNSECURE) provides separate isolated hardware and software. The TOE allows data flow control that is copied and transferred to the SECURE domain from the UNSECURE via a floppy or CD-ROM, but not vice versa. The “Write” function feature of the floppy disk and CD-ROM is disabled on the SECURE domain. Front panel USB ports are not installed on the SECURE domain. See Section 6, User data protection for more detailed information.

2.2.2.2 Mandatory Access Control and Identification and Authentication

A user must be successfully identified prior to gaining access to the TOE and its functions that includes physical access of key #2 that is required to power on the DataVault X4 in the UNSECURE domain. To further access the SECURE domain, the trusted user or Key Administrator needs a Smart Card for authentication and identification. The exception is when the Key Administrator is an administrator of the SECURE domain operating system and the IT environment authentication server. The Key Administrator of the SECURE domain operating system is required to be authenticated before access is granted, but does not require a Smart Card. See Section 6, Mandatory Access Control and Identification and authentication for more detailed information.

2.2.2.3 Security management

The security management functions of the TOE are controlled by the role a user is assigned as well as the keys they are assigned. The three roles that are supported by the TOE are; the Key Administrator, a Trusted user, and a User. See Section 6, Security management for more detailed information.

2.2.2.4 Protection of the TSF

The objects protected by the TSF are the computing hardware, software, and data within a domain. The TSF control access to the domains via the keys and Smart Card the user possess. The TSF also controls the information that can flow between domains. See Section 6, Protection of the TSF for more detailed information.

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

3.1 Threats

T.LOCK The TOE's panels (front, back, and top) maybe compromised by an unauthorized user, therefore exposing the TOE hardware.

T.MEDIAT An unauthorized person may send impermissible information through the TOE, which results in the exploitation of resources on the internal network.

T.NOAUTH An unauthorized person may attempt to bypass the security of the TOE to access and exploit security functions provided by the TOE.

T.SELPRO An unauthorized person may read, modify, or destroy security critical TOE configuration data.

3.2 Assumptions

A.KEYS Access to specific keys and Smart Card is restricted to users, trusted users, and Key Administrators.

A.LOCATE The TOE will be located within controlled access facilities that will prevent unauthorized physical access.

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.NOEVIL The Key Administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator 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 for the TOE, IT Security Objectives for the Environment, or Non-IT Security Objectives for the Environment, reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified, and address the identified assumptions. All of the identified threats, assumptions, and organizational policies are addressed under one of the categories below.

4.1 Security Objectives for the TOE

O.DETECT Unauthorized access to the front and/or back panels of the TOE's cabinet shall be visibly detectable by authorized users. If the Top panel is comprised, an audible alarm will sound.

O.IDAUTH The TOE must identify all users before granting a user access to protected TOE functions.

O.MEDIAT The TOE must mediate the flow of all information from one domain to another domain.

O.SELPRO The TOE must protect itself against attempts by unauthorized users to bypass the TOE security functions.

4.2 Security Objectives for the Non-IT Environment

OE.ASSIGN A record must be maintained that identifies the users who have been assigned keys and the Smart Card.

OE.GUIDAN The TOE must be delivered, installed, administered, and operated in a manner that maintains security.

OE.KEYS Access to key #1 is restricted to the Key Administrator, access to key #2 is restricted to users, trusted users, Key Administrator, access to key #3 is restricted to trusted users and Key Administrators, and access to Smart Card is restricted to trusted users and Key Administrators.

OE.LOCATE The TOE is located within controlled access facilities.

OE.MANAGE There will be one or more competent and trained Key Administrators assigned to manage the TOE and the security of the information it contains.

OE.NOEVIL The Key Administrator is not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.

OE.NOTRST The TOE can only be accessed by Key Administrators, users, and trusted users.

4.3 Security Objectives for the IT Environment

OE.AUTH Trusted users and Key Administrators must have and insert the Smart Card for mandatory access control identification and authentication process for further access to the SECURE domain of the TOE. The exception is when the Key Administrator is an administrator of the SECURE domain operating system and the IT environment authentication server. The Key Administrator of the SECURE domain operating system is required to be authenticated before access is granted, but does not require a Smart Card.

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.

The security functional requirements were drawn from the Part 2 Common Criteria version 2.2.

5.1 TOE Security Functional Requirements

The following table describes the SFRs that are candidates to be satisfied by DataVault X4.

Requirement Class	Requirement Component
FDP: User data protection	FDP_IFC.2: Complete information flow control
	FDP_IFF.1: Simple security attributes
FIA: Identification and authentication	FIA_ATD.1: User attribute definition
	FIA_UID.2a: User identification before any action
FMT: Security management	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_PHP.1: Passive detection of physical attack
	FPT_RVM.1: Non-bypassability of the TSP
	FPT_SEP.1: TSF domain separation

Table 1 TOE Security Functional Components

5.1.1 User data protection (FDP)

5.1.1.1 Complete information flow control (FDP_IFC.2)

FDP_IFC.2.1 The TSF shall enforce the [**multi-domain security policy**] on [

a) **Subjects:**
- **users**

b) **Information:**
- **all computing hardware (e.g. motherboard, drivers, memory, processor, network cable connections)**
- **all software (e.g. operating system, application software)**]

and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP.

5.1.1.2 Simple security attributes (FDP_IFF.1)

FDP_IFF.1.1 The TSF shall enforce the [**multi-domain security policy**] based on the following types of subject and information security attributes: [

a) **Subject security attributes:**
- **Possession of key(s)**
- **Possession of Smart Card**

b) **Information:**
- **Physical domain in which computing hardware and software are installed**
- **Selection of the domain with the/ Keyboard "Scroll/Lock" key and the "domain selector switch" mounted on the front of the TOE**].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

a) **users may access information in the UNSECURE domain if they possess key #2 and the front panel has been unlocked by the Key Administrator with key #1,**

b) **trusted user and Key Administrator may access information in both the UNSECURE and the SECURE domain if they possess key #2 and the front panel has been unlocked by the Key Administrator with key #1, possess the Smart Card, and passes Smart Card mandatory access control and authentication and identification process,**

c) **trusted user and Key Administrator may remove the SECURE hard drive (or replace) if they possess key #3].**

FDP_IFF.1.3 The TSF shall enforce the [**trusted user may copy and transfer data from the UNSECURE domain to the SECURE but not vice versa. The "Write" function on both devices; Floppy Drive and CD ROM are mechanically disabled on the SECURE domain. Only the "Read" function is active on the SECURE domain**].

FDP_IFF.1.4 The TSF shall provide the following [**Key Administrator may access the front and back panels if they possess key #1**].

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [**When the Key Administrator is an administrator of the SECURE domain operating system and the IT environment authentication server, the Key Administrator of the SECURE domain operating system is required to be authenticated before access is granted, but does not require a Smart Card**].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow between domains based on the following rules: [**no additional rules that explicitly deny information flows**].

5.1.2 Identification and authentication (FIA)

5.1.2.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**role, key(s) (#1 and/or #2 and/or #3) and Smart Card possession**].

Application Note: The TSF is hardware that does not store authorized user attributes. A user role is defined by what physical key(s) the person possesses and if the trusted user and Key Administrator possesses a Smart Card and can be successfully authenticated and identified by the use of Smart Card technology.

5.1.2.2 User identification before any action (FIA_UID.2a)

FIA_UID.2a.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 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [**Key Administrator, Trusted User, 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 Passive detection of physical attack (FPT_PHP.1)

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

5.1.4.2 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.

5.1.4.3 TSF domain separation (FPT_SEP.1)

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.2 IT Environment Security Functional Requirements

The following table describes the SFRs that are candidates to be satisfied by DataVault X4 IT Environment.

Requirement Class	Requirement Component
FIA: Identification and authentication	FIA_UAU.2: User authentication before any action
	FIA_UID.2b: User identification before any action

Table 2 IT Environment Security Functional Components

5.2.1 Identification and authentication (FIA)

5.2.1.1 User authentication before any action (FIA_UAU.2)

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.2.1.2 User identification before any action (FIA_UID.2b)

FIA_UID.2b.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 4 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_AUT.1: Partial CM automation
	ACM_CAP.4: Generation support and acceptance procedures
	ACM_SCP.2: Problem tracking CM coverage
ADO: Delivery and operation	ADO_DEL.2: Detection of modification
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.2: Fully defined external interfaces
	ADV_HLD.2: Security enforcing high-level design
	ADV_IMP.1: Subset of the implementation of the TSF
	ADV_LLD.1: Descriptive low-level design
	ADV_RCR.1: Informal correspondence demonstration
	ADV_SPM.1: Informal TOE security policy model
AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance

Requirement Class	Requirement Component
ALC: Life cycle support	ALC_DVS.1: Identification of security measures
	ALC_LCD.1: Developer defined life-cycle model
	ALC_TAT.1: Well-defined development tools
ATE: Tests	ATE_COV.2: Analysis of coverage
	ATE_DPT.1: Testing: high-level design
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_MSU.2: Validation of analysis
	AVA_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.2: Independent vulnerability analysis

Table 3 EAL 4 Assurance Components

5.3.1 Configuration management (ACM)

5.3.1.1 Partial CM automation (ACM_AUT.1)

ACM_AUT.1.1d The developer shall use a CM system.
ACM_AUT.1.2d The developer shall provide a CM plan.
ACM_AUT.1.1c The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.
ACM_AUT.1.2c The CM system shall provide an automated means to support the generation of the TOE.
ACM_AUT.1.3c The CM plan shall describe the automated tools used in the CM system.
ACM_AUT.1.4c The CM plan shall describe how the automated tools are used in the CM system.
ACM_AUT.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.2 Generation support and acceptance procedures (ACM_CAP.4)

ACM_CAP.4.1d The developer shall provide a reference for the TOE.
ACM_CAP.4.2d The developer shall use a CM system.
ACM_CAP.4.3d The developer shall provide CM documentation.
ACM_CAP.4.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.4.2c The TOE shall be labelled with its reference.
ACM_CAP.4.3c The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.
ACM_CAP.4.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.4.5c The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.4.6c The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.4.7c The CM system shall uniquely identify all configuration items.
ACM_CAP.4.8c The CM plan shall describe how the CM system is used.
ACM_CAP.4.9c The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
ACM_CAP.4.10c The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
ACM_CAP.4.11c The CM system shall provide measures such that only authorized changes are made to the configuration items.
ACM_CAP.4.12c The CM system shall support the generation of the TOE.
ACM_CAP.4.13c The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.
ACM_CAP.4.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.3 Problem tracking CM coverage (ACM_SCP.2)

ACM_SCP.2.1d The developer shall provide a list of configuration items for the TOE.

ACM_SCP.2.1c The list of configuration items shall include the following: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST.

ACM_SCP.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 Detection of modification (ADO_DEL.2)

ADO_DEL.2.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.2.2d The developer shall use the delivery procedures.

ADO_DEL.2.1c 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.2.2c The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.2.3c The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

ADO_DEL.2.1e 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 Fully defined external interfaces (ADV_FSP.2)

ADV_FSP.2.1d The developer shall provide a functional specification.

ADV_FSP.2.1c The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.2.2c The functional specification shall be internally consistent.

ADV_FSP.2.3c The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

ADV_FSP.2.4c The functional specification shall completely represent the TSF.

ADV_FSP.2.5c The functional specification shall include rationale that the TSF is completely represented.

ADV_FSP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.2 Security enforcing high-level design (ADV_HLD.2)

ADV_HLD.2.1d The developer shall provide the high-level design of the TSF.

ADV_HLD.2.1c The presentation of the high-level design shall be informal.

ADV_HLD.2.2c The high-level design shall be internally consistent.

ADV_HLD.2.3c The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5c 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.2.6c The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8c The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9c The high-level design shall describe the separation of the TOE into TSP enforcing and other subsystems.

ADV_HLD.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.2.2e 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 Subset of the implementation of the TSF (ADV_IMP.1)

ADV_IMP.1.1d The developer shall provide the implementation representation for a selected subset of the TSF.

ADV_IMP.1.1c The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.1.2c The implementation representation shall be internally consistent.

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

ADV_IMP.1.2e The evaluator shall determine that the least abstract TSF representation provided is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.4 Descriptive low-level design (ADV_LLD.1)

ADV_LLD.1.1d The developer shall provide the low-level design of the TSF.

ADV_LLD.1.1c The presentation of the low-level design shall be informal.

ADV_LLD.1.2c The low-level design shall be internally consistent.

ADV_LLD.1.3c The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4c The low-level design shall describe the purpose of each module.

ADV_LLD.1.5c The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6c The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7c The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8c The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9c The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_LLD.1.10c The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

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

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

5.3.3.5 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.

5.3.3.6 Informal TOE security policy model (ADV_SPM.1)

ADV_SPM.1.1d The developer shall provide a TSP model.

ADV_SPM.1.2d The developer shall demonstrate correspondence between the functional specification and the TSP model.

ADV_SPM.1.1c The TSP model shall be informal.

ADV_SPM.1.2c The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.1.3c The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.1.4c The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

ADV_SPM.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 behavior 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 behavior 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 Life cycle support (ALC)

5.3.5.1 Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1d The developer shall produce development security documentation.

ALC_DVS.1.1c The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2c The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

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

ALC_DVS.1.2e The evaluator shall confirm that the security measures are being applied.

5.3.5.2 Developer defined life-cycle model (ALC_LCD.1)

ALC_LCD.1.1d The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2d The developer shall provide life-cycle definition documentation.

ALC_LCD.1.1c The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2c The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

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

5.3.5.3 Well-defined development tools (ALC_TAT.1)

ALC_TAT.1.1d The developer shall identify the development tools being used for the TOE.

ALC_TAT.1.2d The developer shall document the selected implementation-dependent options of the development tools.

ALC_TAT.1.1c All development tools used for implementation shall be well-defined.

ALC_TAT.1.2c The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.1.3c The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

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

5.3.6 Tests (ATE)

5.3.6.1 Analysis of coverage (ATE_COV.2)

ATE_COV.2.1d The developer shall provide an analysis of the test coverage.

ATE_COV.2.1c The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2c The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

ATE_COV.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6.2 Testing: high-level design (ATE_DPT.1)

ATE_DPT.1.1d The developer shall provide the analysis of the depth of testing.

ATE_DPT.1.1c The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

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

5.3.6.3 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.

5.3.6.4 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.

5.3.7 Vulnerability assessment (AVA)

5.3.7.1 Validation of analysis (AVA_MSU.2)

AVA_MSU.2.1d The developer shall provide guidance documentation.

AVA_MSU.2.2d The developer shall document an analysis of the guidance documentation.

AVA_MSU.2.1c The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.2.2c The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.2.3c The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.2.4c The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.2.5c The analysis documentation shall demonstrate that the guidance documentation is complete.

AVA_MSU.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.2.2e The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.2.3e The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

AVA_MSU.2.4e The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.

5.3.7.2 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.

5.3.7.3 Independent vulnerability analysis (AVA_VLA.2)

AVA_VLA.2.1d The developer shall perform a vulnerability analysis.

AVA_VLA.2.2d The developer shall provide vulnerability analysis documentation.

AVA_VLA.2.1c The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.

AVA_VLA.2.2c The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.

AVA_VLA.2.3c 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.2.4c The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

AVA_VLA.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.2.2e The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

AVA_VLA.2.3e The evaluator shall perform an independent vulnerability analysis.

AVA_VLA.2.4e The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

AVA_VLA.2.5e The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low attack potential.

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 provides complete information flow control between security domains where each domain provides isolated hardware and software.

Each security domain includes its own hardware as follows: motherboard, hard drive, controllers, memory, processor, network interface cards, and network port connections. They share no common components with the exception of the keyboard, mouse, case with power supply, and K&M switch. When the TOE switches between domains all data access via the keyboard and mouse is suspended in the domain that is being exited. The cursor on the exited monitor remains stationary and the keyboard is non-functional in the exited domain. When the exited domain is again selected, data processing continues at the point where the domain was last exited. No information flows from one domain to another before, during, or after a domain switch. The only way to transfer data and information from the UNSECURE to the SECURE domains is through the use of a floppy disk or CD/ROM by a trusted user. The Read/Write function of the floppy on the UNSECURE domain is enabled. The Write function of the Floppy Drive and DVD or CD/ROM on the SECURE domain is mechanically disabled so data cannot be copied onto a floppy disk or CD from the SECURE network or SECURE removable hard drive. This prevents data theft from the SECURE domain, even when a trusted user is accessing it. This configuration assures that no data can flow from one domain to the other because each domain is totally isolated and separate from the other.

The DataVault X4 enforces the following policies:

1. Users cannot access the DataVault X4 workstation without a Key Administrator unlocking the front panel cover with key #1. Once the Key administrator has unlocked the front panel, a user must posses a valid key #2 to turn on and boot the system. This grants the user access to the UNSECURE domain.
2. To gain access to the SECURE domain, a trusted user or Key Administrator must possess key #2 and possess a Smart card, and pass the Smart Card mandatory access control identification and authentication process. A user may toggle and attempt to access the SECURE domain, though access is not granted to user unless they possess a Smart card and can pass the Smart Card mandatory access control identification and authentication process. The exception is when the Key Administrator is an administrator of the SECURE domain operating system and the IT environment authentication server. The Key Administrator of the SECURE domain operating system is required to be authenticated before access is granted, but does not require a Smart Card.
3. Only a trusted user or Key Administrator that possess key #3 can unlock and remove the SECURE removable hard drive. To remove or replace the hard drive, the trusted user or Key administrator must possess key #3.
4. The SECURE domain floppy drive is Read-Only so even the trusted user or Key Administrator cannot copy and remove or transport data from the SECURE domain. A user can however copy data from the UNSECURE domain onto a floppy disk or CD-ROM.
5. Only a Key Administrator with key #1 can access the TOE's internal components, interfaces and network connections, and the case open alarm lock.

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

- FDP_IFC.2: The TOE provides an information flow policy between users and the physical domains of the TOE.
- FDP_IFF.1: The TOE provides a single domain information flow policy that defines the rules based upon the attributes defined in the SFR.

6.1.2 Mandatory Access Control and Identification and authentication

A user must be successfully identified prior to gaining access to the TOE and its functions with the On/Off key #2. The TSF is hardware that does not store user attributes. A user role is defined by the physical keys and Smart card the user possesses and if the user can be successfully identified and authenticated by Smart Card technology. The exception is when the Key Administrator is an administrator of the SECURE domain operating system and the IT environment authentication server. The Key Administrator of the SECURE domain operating system is required to be authenticated before access is granted, but does not require a Smart Card.

Mandatory Access Control and Identification and authentication includes:

Front Panel Key - There is a physical key that unlocks the front panel of a specific DataVault X4. Until the Key Administrator using key #1 unlocks the front panel, the TOE is inaccessible and inoperable. All roles that are provided access to a specific DataVault X4 must have the front panel open.

Back Panel Key – All network cables and peripheral cabling into the TOE are connected onto the back of the TOE and these are protected by a rear lockable panel cover. No access is afforded to cable connections without the possession of a Front and Back Panel Key #1. Only a Key administrator has access to this key, therefore if a person has a Front and Back Panel Key #1 in their possession, this identifies the person in the group of key administrators assigned to control access to a specific number of DataVault X4's.

Operational key - All users that are granted access to use a specific DataVault X4 must have key #2 to turn on the system, which boots the TOE to the UNSECURE domain.

SECURE hard drive key – To remove the SECURE hard drive, the trusted user or Key Administrator must possess key #3.

Smart Card - To further access and view the SECURE domain the user (trusted user or Key Administrator) needs a Smart Card for authentication and identification. Although Smart Card authentication is not part of the TOE, the enforcement of the decision returned from Smart card authentication is enforced by the TOE when allowing access to the SECURE domain. The exception is when the Key Administrator is an administrator of the SECURE domain operating system and the IT environment authentication server. The Key Administrator of the SECURE domain operating system is required to be authenticated before access is granted, but does not require a Smart Card.

The Mandatory Access Control Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1: The TOE recognizes the security attributes belonging to a user as role, which is determined by the front panel key # 1, the On/Off key #2, the ability to remove the SECURE hard drive with key #3, and the possession of a Smart Card.
- FIA_UID.2a: The TOE offers no TSF-mediated functions until the user is identified.

6.1.3 Security management

Since the TOE Security Functions (TSF) only control mechanical, and electromechanical, security management focuses on installation of the TOE. Once the TOE is installed and configured, the only management is to install the network cablings on both domains and to control the distribution of the key #1, key #2, key #3, and the Smart Card for further accessing the SECURE domain that has mandatory access control identification and authentication process for trusted user and Key Administrator identification and authentication. The Key Administrator is responsible for maintaining, issuing, and deleting keys and the Smart Card. The Key Administrator may also be the administrator for the IT environment authentication server responsible for creating and maintaining the user accounts and Smart Cards required for TOE identification and authentication.

The TOE supports the notion of roles. Roles are determined by the keys and the Smart Card the user possess. The three roles that are supported are:

- Key Administrator

- Trusted user
- User.

Key Administrator is a person who

- Possesses a physical key #1 to the front and back panel of the TOE so that devices and network cablings can be maintained and controlled
- Possesses a physical key #2 to turn On/Off each DataVault X4 and deactivate or activate the "open case alarm" located inside the back panel of the TOE. Each key # 2 is specific to each DataVault X4
- Possesses an physical key #3 to remove the SECURE hard drive or install a SECURE hard drive (or blank drive),
- Possesses a valid Smart Card to access all SECURE domains
- Distributes keys and Smart Card to users and trusted users

A trusted user possesses the same keys as the Key Administrator except for the front/back panel key #1; therefore the trusted user cannot modify network connections. Trusted users also possess Smart Card. Trusted users can remove or replace SECURE hard drives if they possess key #3.

A user may only have key #2 to switch the system on (off), which automatically boots the computer to the UNSECURE domain.

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

- FMT_SMR.1: The TOE supports three roles; Key Administrator, Trusted User, and User.

6.1.4 Protection of the TSF

The TOE provides a locked front panel cover and a locked back panel cover. Both the front and back panel covers are locked when the TOE is not in use to protect entry into the cabinet. To remove hardware through the front of the TOE after the front panel has been locked requires forced entry through the front of the cabinet, which subsequently provides evidence of forced entry. Modifying connected hardware or network connections requires modifying cable connections to the back of the TOE that is protected by the back panel cover. The back panel cover is locked and the only way to change connected hardware or network connections is either force entry beyond the panel or by cutting and splicing wire connections. Either method provides physical evidence of unauthorized entry and attack.

The objects protected by the TSF are the computing hardware, software, and data within a domain. The TSF control access to the domains via the keys and Smart Card the user possess. The TSF also controls the information that can flow between domains. No information can flow between the SECURE and UNSECURE domains, since no shared devices and connections are provided between domains except the keyboard, mouse, case with power supply, and K&M switch. The only way data can pass between the SECURE and UNSECURE domain is via a floppy disk or CD-ROM by a trusted user or Key Administrator. The Read/Write function of the floppy on the UNSECURE domain is enabled. The Write function of the Floppy Drive or CD/ROM on the SECURE domain is mechanically disabled so data cannot be copied onto a floppy disk or CD-ROM from the SECURE network or SECURE removable hard drive. This prevents data theft from the SECURE domain, even when a trusted user is accessing it. In summary, data can be transferred from the UNSECURE domain to the SECURE by a trusted user or Key Administrator but not vice-versa. The Key Administrator can export data from the SECURE domain by opening the back panel and accessing the mass storage device port.

The TSF cannot be circumvented because the TSF must be invoked before access to a domain is provided. The TSF enforces separation between the security domains based on the user's security attributes and controls access to the SECURE domain even after it is powered on by a user. For instance, when the TOE switches between domains all data access via the keyboard and mouse is suspended in the domain that is being exited. The cursor on the exited monitor remains stationary and the keyboard is non-functional in the exited domain. When the exited domain is again selected, data processing continues at the point where the domain was last exited. No information flows from one domain to another before, during, or after a domain switch. In addition, when a user toggles between the domains, only a trusted user or Key Administrator that possess a Smart card, and pass the Smart Card mandatory access control identification and authentication process can access data in the SECURE domain. The exception is when the Key Administrator is an administrator of the SECURE domain operating system and the IT environment authentication server. The Key Administrator of the SECURE domain operating system is required to be authenticated before access is granted, but does not require a Smart Card.

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

- FPT_PHP.1: The TOE provides physical protection via the front and back panels of the TOE's cabinet.
- FPT_RVM.1: There is no means to bypass the TOE's security policies.
- FPT_SEP.1: The TSF enforces separation between the security domains based on the user's security attributes.

6.2 TOE Security Assurance Measures

6.2.1 Configuration management

A description of the configuration management system used by Secutor Systems, Inc. will be provided with a configuration list. The configuration management measures applied by Secutor Systems, Inc. ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. Secutor Systems, Inc. ensures changes to the implementation representation are controlled with the support of automated tools and that TOE associated configuration item modifications are properly controlled. Secutor Systems, Inc. performs configuration management on the TOE implementation representation, design documentation, tests and test documentation, user and administrator guidance, delivery and operation documentation, life-cycle documentation, vulnerability analysis documentation, configuration management documentation, and security flaws.

The Configuration management assurance measure satisfies the following EAL 4 assurance requirements:

- ACM_AUT.1
- ACM_CAP.4
- ACM_SCP.2

6.2.2 Delivery and operation

Secutor Systems, Inc. will provide delivery documentation and procedures to identify the TOE, allow detection of unauthorized modifications of the TOE and installation and generation instructions at start-up. Secutor Systems, Inc.'s delivery procedures describe all applicable procedures to be used to detect modification to the TOE. Secutor Systems, Inc. also provides documentation that describes the steps necessary to install DataVault X4 in accordance with the evaluated configuration.

The Delivery and operation assurance measure satisfies the following EAL 4 assurance requirements:

- ADO_DEL.2
- ADO_IGS.1

6.2.3 Development

Secutor Systems, Inc. has a document that will be provided that describes all facets of the design of the TOE. In particular, they have a functional specification that describes the accessible TOE interfaces; a high-level design that decomposes the TOE architecture into subsystems and describes each subsystem and their interfaces; a low-level design that further decomposes the TOE architecture into modules and describes each module and their interfaces; and, correspondence documentation that explains how each of the design abstractions correspond from the TOE summary specification in the Security Target to the actual implementation of the TOE. Furthermore, Secutor Systems, Inc. has a security model that describes each of the security policies implemented by DataVault X4. Of course, the implementation of the TOE itself is also available as necessary.

The Development assurance measure satisfies the following EAL 4 assurance requirements:

- ADV_FSP.2
- ADV_HLD.2
- ADV_IMP.1
- ADV_LLD.1
- ADV_RCR.1
- ADV_SPM.1

6.2.4 Guidance documents

Secutor Systems, Inc. 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.

The Guidance documents assurance measure satisfies the following EAL 4 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Life cycle support

Secutor Systems, Inc. ensures the adequacy of the procedures used during the development and maintenance of the TOE through the use of a comprehensive life-cycle management plan that will be provided. Secutor Systems, Inc. includes security controls on the development environment that are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure the secure operation of the TOE. Secutor Systems, Inc. achieves this through the use of a documented model of the TOE life cycle and well-defined development tools that yield consistent and predictable results.

The Life cycle support assurance measure satisfies the following EAL 4 assurance requirements:

- ALC_DVS.1
- ALC_LCD.1
- ALC_TAT.1

6.2.6 Tests

Secutor Systems, Inc. has a test plan that will be provided that describes how each of the necessary security functions is tested, along with the expected test results. Secutor Systems, Inc. has documented each test as well as an analysis of test coverage and depth demonstrating that the security aspects of the design evident from the functional specification and high-level design are appropriately tested. Secutor Systems, Inc. executes the test on a regular basis to demonstrate that the tests have been applied and that the TOE operates as designed. The actual results will also be provided.

The Tests assurance measure satisfies the following EAL 4 assurance requirements:

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

6.2.7 Vulnerability assessment

The TOE administrator and user guidance documents describe the operation of DataVault X4 and how to maintain a secure state. These guides also describe all necessary operating assumptions and security requirements outside the scope of control of the TOE. They have been developed to serve as complete, clear, consistent, and reasonable administrator and user references. Furthermore, Secutor Systems, Inc. has conducted a misuse analysis and documented the findings that demonstrate the provided guidance is complete.

Secutor Systems, Inc. has conducted a strength of function analysis to identify and analyze permutational or probabilistic security mechanisms implemented in the TOE. The ST does not specify any security functional requirements or security functions that involve permutational or probabilistic mechanisms. Therefore, an overall strength of function claim is not applicable, and the assurance requirements of AVA_SOF.1 are vacuously satisfied.

Secutor Systems, Inc. performs regular vulnerability analyses of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE. The analyses was documented and will be provided.

The Vulnerability assessment assurance measure satisfies the following EAL 4 assurance requirements:

- AVA_MSU.2
- AVA_SOF.1
- AVA_VLA.2

7. Protection Profile Claims

This Security Target makes no Protection Profile claim.

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 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.

	T.LOCK	**T.MEDIAT**	**T.NOAUTH**	**T.SELPRO**	**A.KEYS**	**A.LOCATE**	**A.MANAGE**	**A.NOEVIL**
O.DETECT	X							
O.IDAUTH			X					
O.MEDIAT		X						
O.SELPRO				X				
OE.ASSIGN					X			
OE.GUIDAN							X	
OE.KEYS					X			
OE.LOCATE						X		
OE.MANAGE							X	
OE.NOEVIL								X
OE.NOTRST			X			X		
OE.AUTH			X					

Table 4 Environment to Objective Correspondence

8.1.1.1 T.LOCK

The TOE's panels (front, back, and top) maybe compromised by an unauthorized user, therefore exposing the TOE hardware.

This Threat is satisfied by ensuring that:

- O.DETECT: This security objective requires that if the front and/or back panels of the TOE's cabinet have been compromised, it shall be visibly detectable by an authorized user. If the Top panel has been compromised, the open case alarm omits a loud sound if accessed without disarming the case alarm.

8.1.1.2 T.MEDIAT

An unauthorized person may send impermissible information through the TOE, which results in the exploitation of resources on the internal network.

This Threat is satisfied by ensuring that:

- O.MEDIAT: This security objective requires that the TOE appropriately mediate all information that passes through the domains.

8.1.1.3 T.NOAUTH

An unauthorized person may attempt to bypass the security of the TOE to access and exploit security functions provided by the TOE.

This Threat is satisfied by ensuring that:

- O.IDAUTH: This security objective requires that users be uniquely identified and authenticated before accessing the TOE.
- OE.AUTH: This security objective requires that users be uniquely identified and authenticated before accessing the TOE
- OE.NOTRST: The TOE can only be accessed by key administrators, users, and trusted users; hence authorized users.

8.1.1.4 T.SELPRO

An unauthorized person may read, modify, or destroy security critical TOE configuration data.

This Threat is satisfied by ensuring that:

- O.SELPRO: This security objective requires that the TOE protect itself from attempts to bypass with TOE security functions.

8.1.1.5 A.KEYS

Access to specific keys and the Smart Card is restricted to users, trusted users, and Key Administrators.

This Assumption is satisfied by ensuring that:

- OE.ASSIGN: A record is maintained to track users who have been assigned keys and the Smart Card.
- OE.KEYS: Access to the keys and Smart Card is restricted to specific users.

8.1.1.6 A.LOCATE

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

This Assumption is satisfied by ensuring that:

- OE.LOCATE: The TOE is physically secure.
- OE.NOTRST: The TOE can only be accessed by key administrators, users, and trusted users; hence authorized users.

8.1.1.7 A.MANAGE

There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

This Assumption is satisfied by ensuring that:

- OE.MANAGE: There will be one or more competent and trained individuals assigned to manage the TOE and the security of the information it contains.
- OE.GUIDAN: This non-IT security objective requires that those responsible for the TOE ensure that it is delivered, installed, administered, and operated in a secure manner

8.1.1.8 A.NOEVIL

The Key Administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.

This Assumption is satisfied by ensuring that:

- OE.NOEVIL: Key administrators are non-hostile and follow all administrator guidance.

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.DETECT	**O.IDAUTH**	**O.MEDIAT**	**O.SELPRO**	**OE.AUTH**
FDP_IFC.2			X		
FDP_IFF.1			X		
FIA_ATD.1		X			
FIA_UID.2a		X			
FMT_SMR.1					
FPT_PHP.1	X				
FPT_RVM.1				X	
FPT_SEP.1				X	
FIA_UAU.2					X
FIA_UID.2b					X

Table 5 Objective to Requirement Correspondence

8.2.1.1 O.DETECT

Unauthorized access to the front and/or back panels of the TOE's cabinet shall be detectable by authorized users.

This TOE Security Objective is satisfied by ensuring that:

- FPT_PHP.1: An authorized user shall be able to detect unauthorized access to the TOE's front and/or back panels.

8.2.1.2 O.IDAUTH

The TOE must identify all users before granting a user access to protected TOE functions.

This TOE Security Objective is satisfied by ensuring that:

- FIA_ATD.1: The TOE is required to manage user attributes.
- FIA_UID.2a: The TOE is required to identify users before allowing access to protected TSF functions.
- FMT_SMR.1: The TOE is required to define a role. The role is determined by the keys and Smart Card the user possess

8.2.1.3 O.MEDIAT

The TOE must mediate the flow of all information from one domain to another domain.

This TOE Security Objective is satisfied by ensuring that:

- FDP_IFC.2: The TOE is required to mediate information flowing through the TOE.
- FDP_IFF.1: The TOE is required to enforce information flow rules defined in the multi-domain security policy.

8.2.1.4 O.SELPRO

The TOE must protect itself against attempts by unauthorized users to bypass the TOE security functions.

This TOE Security Objective is satisfied by ensuring that:

- FPT_RVM.1: The TOE is required to ensure that its functions cannot be bypassed.
- FPT_SEP.1: The TOE must protect itself against attempts by unauthorized users to bypass the TOE security functions.

8.2.1.5 OE.AUTH

Trusted users and Key Administrators must have and insert the Smart Card for mandatory access control identification and authentication process for further access to the SECURE domain of the TOE. The exception is when the Key Administrator is an administrator of the SECURE domain operating system and the IT environment authentication server. The Key Administrator of the SECURE domain operating system is required to be authenticated before access is granted, but does not require a Smart Card.

This IT Environment Security Objective is satisfied by ensuring that:

- FIA_UAU.2: The IT environment is required to authenticate users before allowing access to protected TSF functions.
- FIA_UID.2b: The IT environment is required to identify users before allowing access to protected TSF functions.

8.3 Security Assurance Requirements Rationale

This ST contains the assurance requirements from the CC EAL4 assurance package and is based on good commercial development practices. This ST has been developed for a generalized environment with a medium level of risk to the assets. The security environment assumes physical protection and the TOE itself offers only a very limited interface and can only be configured during initialization, offering essentially no opportunity for an attacker to subvert the security policies without physical access. As such, it is believed that EAL4 provides an appropriate level of assurance in the security functions offered by the TOE.

8.4 Strength of Functions Rationale

The TOE does not specify any security functional requirements or implement any security functions that involve permutational or probabilistic mechanisms. Therefore, an overall strength of function claim is not applicable.

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_IFC.2	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 and FMT_MSA.3	FDP_IFC.2 and FMT_MSA.3
FIA_ATD.1	none	none
FIA_UID.2a	none	none
FMT_SMR.1	FIA_UID.1	FIA_UID.2a
FPT_PHP.1	none	none
FPT_RVM.1	none	none
FPT_SEP.1	none	none
FIA_UAU.2	FIA_UID.1	FIA_UID.2b
FIA_UID.2b	none	none

Table 6 Requirement Dependency Rationale

For FDP_IFF.1 requirement, the CC identifies the following dependency; FMT_MSA.3. The dependencies for this requirement are not applicable for this TOE. Following is the justification for not including these requirements:

- FMT_MSA.3 – The FMT_MSA.3.1 requirement is a dependency of the FDP_IFF.1 requirement to support the management of security attributes that are used to enforce the SFP. The security attributes that are utilized to enforce the SFP are physical keys and Smart Card. Neither the TOE nor the IT environment can provide enforcement of physical items that are utilized to determine access. Therefore, the Non-IT Environment provides the control and management of the security attributes.

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 7 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**
FDP_IFC.2	X			
FDP_IFF.1	X			

	User data protection	Identification and authentication	Security management	Protection of the TSF
FIA_ATD.1		X		
FIA_UID.2a		X		
FMT_SMR.1			X	
FPT_PHP.1				X
FPT_RVM.1				X
FPT_SEP.1				X

Table 7 Security Functions vs. Requirements Mapping

8.8 PP Claims Rationale

See Section 7, Protection Profile Claims.