

Multistate Tax Commission

Secure Communications Requirements

Version 4.0

July 12, 2007

The logo for e.magination, featuring the word "e.magination" in a lowercase, italicized, sans-serif font. The "e" is smaller and positioned to the left of "magination". The logo is centered within a dark gray rectangular background.

CORPORATE HEADQUARTERS

1030 Hull Street

The Cascade Building – Suite 300

Baltimore, MD 21230

410.234.1500

REVISION HISTORY

Date	Version	Description	Author
7-06-06	1.0	First Draft	Rachel Foster
7-10-06	2.0	Second Draft	Rachel Foster
8-02-06	2.1	Third Draft	Rachel Foster
07-12-07	2.2	Fourth Draft	Rachel Foster

TABLE OF CONTENTS

1.0	INTRODUCTION	1
1.1	OVERVIEW	1
1.2	DOCUMENT OVERVIEW.....	1
2.0	BUSINESS PROCESS REVIEW	2
2.1	AUDIT USER ANALYSIS.....	2
2.2	AUDIT HIGH-LEVEL BUSINESS PROCESS DIAGRAM	4
2.3	BUSINESS PROCESS REQUIREMENTS.....	5
2.4	LITIGATION USER ANALYSIS	6
2.5	LITIGATION HIGH-LEVEL BUSINESS PROCESS DIAGRAM.....	7
2.6	LITIGATION BUSINESS PROCESS REQUIREMENTS.....	7
2.7	NEXUS/ VOLUNTARY DISCLOSURE USER ANALYSIS.....	8
2.8	NEXUS/ VOLUNTARY DISCLOSURE HIGH-LEVEL BUSINESS PROCESS DIAGRAM	9
2.9	NEXUS/ VOLUNTARY DISCLOSURE BUSINESS PROCESS REQUIREMENTS	10
3.0	SECURE COMMUNICATIONS REQUIREMENTS	11
3.1	FRAMEWORK FUNCTIONAL REQUIREMENTS	11
3.1.1	Operational Requirements.....	11
3.1.2	Physical Requirements	13
3.1.3	Cyber Requirements.....	13
4.0	REGULATIONS AND GUIDELINES DISCUSSION.....	16
5.0	SECURE COMMUNICATIONS SOLUTIONS.....	17
5.1.1	Introduction.....	17
5.1.2	Option 1: Secure FTP.....	17
5.1.3	Option 2: Secure Portal	18
6.0	APPENDIX 1: POLICY AND PROCESS LISTS	20
6.1	POLICY AND PROCESS LISTS FOR MTC	20
6.1.1	Personnel Security Policy:	20
6.1.2	User ID & Password Policy (including identification and authentication):.....	20
6.1.3	Authentication.....	22
6.1.4	Authorization	23
6.1.5	Awareness & Training Policy:.....	24
6.1.6	Incident Response and Reporting Policy:	24
6.1.7	Maintenance Policy:.....	25
6.1.8	Configuration Management Policy:	25

6.1.9	Acceptable Use Policy:	26
6.1.10	Confidentiality Policy:	27
6.1.11	Security Assessment Policy:	27
6.1.12	Contingency Planning:	27
6.1.13	Risk Assessment:.....	28
6.1.14	Access Control Policy:	28
6.1.15	Audit Procedures:	29
6.1.16	System & Information Integrity Policy:	31

1.0 INTRODUCTION

1.1 OVERVIEW

The underlying critical requirement for MTC and the member states is that MTC applications and systems provide a framework for secure communications. The secure communications framework will be focused on the storage and transmission of taxpayer confidential information. Everyone involved in MTC operations need to be assured that documents transferred and stored within the system are secured against unauthorized disclosure. Additionally, everyone must be assured that the systems put in place will meet state and federal standards for secure communications. A plan to implement these requirements, along with the business processes that will monitor and maintain them is critical.

1.2 DOCUMENT OVERVIEW

The document is focused on capturing the requirements for secure communications between the MTC and constituents. It includes the following:

- Business Process Review
- Requirements for Secure Communications
- Regulations Discussion

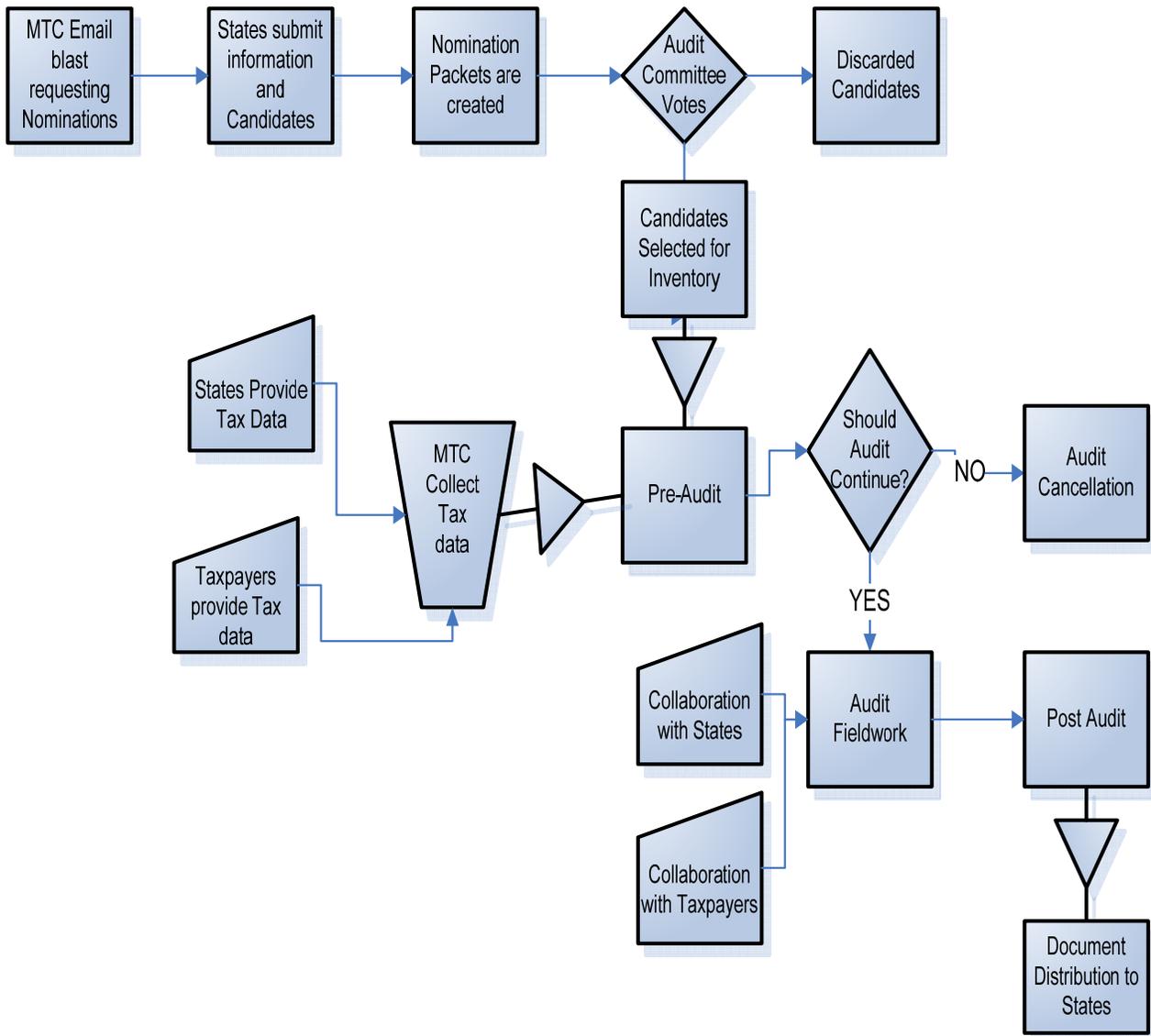
2.0 BUSINESS PROCESS REVIEW

2.1 AUDIT USER ANALYSIS

	 Audit
High Level Process	<p>Process begins MTC sends an email blast to the states requesting nominations for audit candidates.</p> <ul style="list-style-type: none"> ○ Each state will mail in their nominations. ○ States send in the Tax Return or documentation on each candidate manually. Then MTC manually compiles that information into packages. ○ The states research the information and then the Audit Committee will vote for each candidate ○ During the Audit Committee meeting, members determine the top list of candidates, those with the most votes. ○ This top list will become the Audit Inventory. ○ The inventory information is stored in an Access Database. ○ Nexus could also discover an audit candidate through their investigations. It would be submitted to the Audit Committee for approval and then added to the Inventory Database. ○ Then the audit is released to the Audit supervisors who will assign an auditor. ○ Audit authorization forms are sent to each state. States will mail back the audit authorization form and additional information ○ During this stage or during pre-audit, an audit may be cancelled for a number of reasons. It may not be a good audit candidate, not enough state participation, etc. A notice will be sent to the states with explanations. ○ During Pre-Audit, the auditors perform research tasks and collect information from the states and the taxpayers. ○ Audit Fieldwork- communications between auditor, states, and taxpayers and Internal Documentation collaborations ○ Sales Tax Audits could utilize electronic audits. ○ Post Audit Process requires a dissemination of the finished product. Today the documents are sent out manually.
Goals	<ul style="list-style-type: none"> ○ A vehicle for secure communications between states, taxpayers, and MTC. ○ Automating the processes: Nomination, Inventory, Pre-Audit, Fieldwork, and Post Audit ○ Providing a Database that could be leveraged for other projects, reports, etc. ○ Provide a vehicle for secure collaboration. ○ Automating internal processes: Timesheets, status reports, etc.

	<p><u>Things to be automated:</u></p> <ul style="list-style-type: none">• Versioning documents (automatic versioning)• Storing documents• Audit External and Internal processes• Central database where all information is stored.
--	---

2.2 AUDIT HIGH-LEVEL BUSINESS PROCESS DIAGRAM



2.3 BUSINESS PROCESS REQUIREMENTS

The Current Audit Process is comprised of the following phases: Nomination, Inventory, Pre- Audit Preparation, Audit Field Work, and Post-Audit. For the Secure Communications Plan, MTC is reviewing the current process, evaluating its effectiveness, and determining areas of automation.

SR-01 Data Types

The Audit Process involves the following types of data: taxpayer confidential data, state tax forms and information, federal tax forms and information, Federal Identification Numbers, statistical data, corporate income information, and sales tax data.

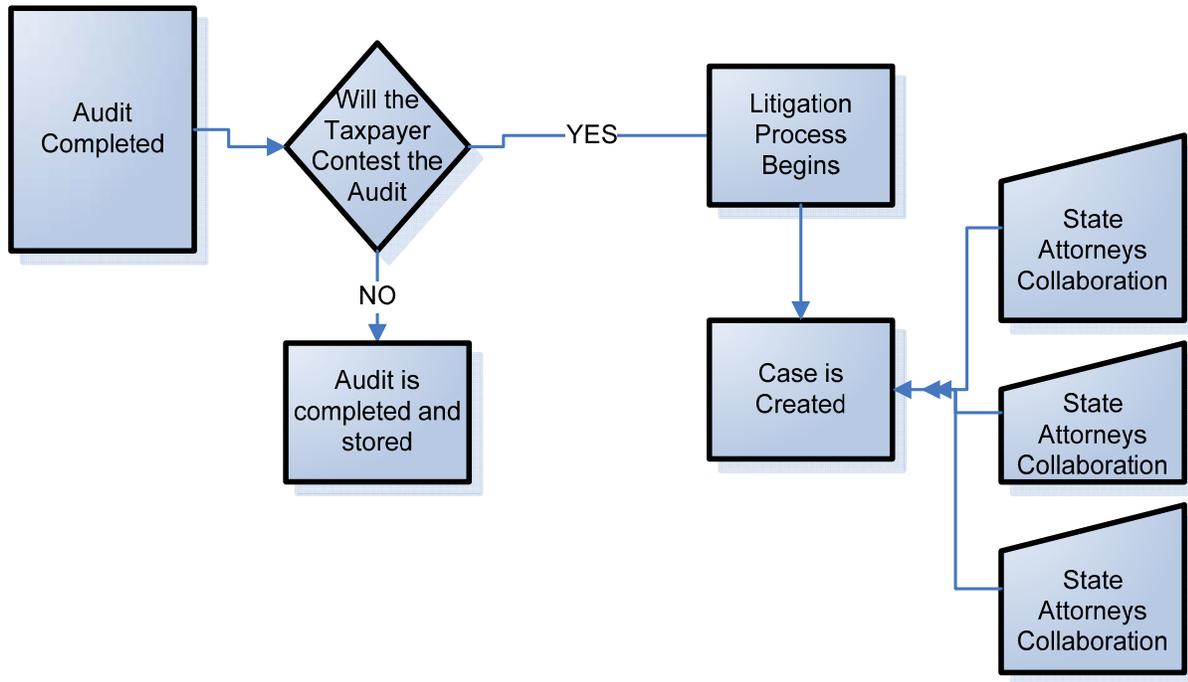
SR-02 Business Process to be put in place

- Access Management: User Validation and Authentication Process
- Roles Management
- Document Management

2.4 LITIGATION USER ANALYSIS

	 Litigation
High Level Process	<p>Process begins when a taxpayer contests an Audit or if member states attorneys would like to collaborate on a particular case or taxpayer.</p> <ul style="list-style-type: none"> ○ Attorneys would need to be able to access Audit information on a taxpayer. ○ Attorneys collaborate on state cases
Goals	<ul style="list-style-type: none"> ○ The ability to leverage the Audit Database ○ Be able to build on the audit data and input case data ○ A database of Expert Witnesses ○ A database of legal briefs ○ The ability to securely collaborate, share documents, request information, schedule regular teleconferences or meetings ○ The ability to search for information by issue or case and pull lists and reports. ○ Would like to have a presentation on the secure solution for the user community. <p><u>Things to be automated:</u></p> <ul style="list-style-type: none"> ● Versioning documents (automatic versioning) ● Storing documents ● Central database where all information is stored.

2.5 LITIGATION HIGH-LEVEL BUSINESS PROCESS DIAGRAM



2.6 LITIGATION BUSINESS PROCESS REQUIREMENTS

The Litigation Process begins after Post-Audit. It leverages information captured during the Audit Process.

Data Types

The Litigation Process involves the following types of data: legal briefs, case information, taxpayer confidential data, state tax forms and information, federal tax forms and information, Federal Identification Numbers, statistical data, corporate income information, and sales tax data.

SR-03 Business Process to be put in place

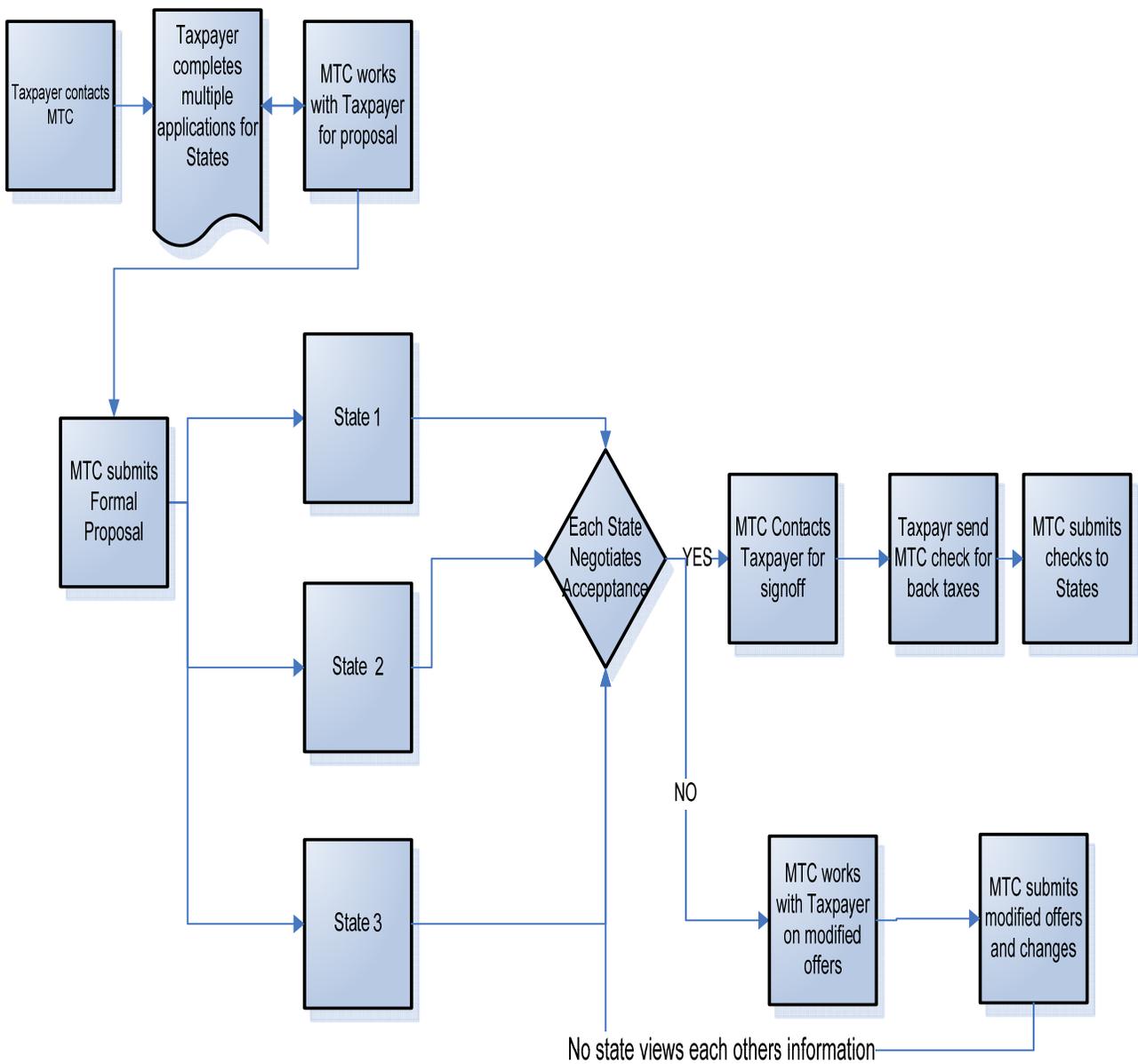
- Access Management: User Validation and Authentication Process
- Roles Management
- Document Management

2.7 NEXUS/ VOLUNTARY DISCLOSURE USER ANALYSIS

	 Nexus: Voluntary Disclosure
High Level Process	<p>Process begins when a Taxpayer contacts MTC and would like to make a confidential disclosure to some or all States on a certain kind of tax, normally sales or use tax or corporate franchise tax.</p> <ul style="list-style-type: none"> ○ Taxpayer works with MTC personnel, who answer the Taxpayer’s questions and makes a formal proposal to the State for disclosure. ○ Have an application where the Taxpayer fills in the information to be put into the proposal (usually the application has the same questions; some States do not allow information to be put into writing, so the questions can vary – this could cause MTC to speak to the Taxpayer on the phone). ○ Eventually staff will get a draft proposal in shape, Taxpayer signs off or makes modifications, sent off to States, and then States would decide whether or not to reject or make a counter offer. Keep track of who is supposed to go next in the process ○ No State at any point can know what other States are doing unless the Taxpayer approves this. If a State rejects an offer, they will never know the identity of the Taxpayer. ○ States will let MTC know if they accept or reject the proposal. A State will usually say if the Taxpayer does A, B, & C, then we will accept it. If the Taxpayer agrees to A, B, & C, then the State and the Taxpayer sign off on it. ○ MTC gets checks for back taxes and registration of Taxpayer. This is usually how MTC and the participating States discover the identity of the Taxpayer. ○ Any payments are then made to the States by the Taxpayer.
Goals	<ul style="list-style-type: none"> ○ An Online Application for Voluntary Disclosure that would be submitted through the Public website. ○ The same application would be used for proposals to various States, but would allow a separation of information for each State (right now, this process is tedious and manual). ○ A secure means of communicating with the Taxpayer and the States where no information is revealed concerning identity or terms. ○ Would like to provide a vehicle for Taxpayer and States to communication anonymously to one another through the MTC ○ Could teleconference (bridge) the Taxpayer with the State through MTC. <p><u>Things to be automated:</u></p> <ul style="list-style-type: none"> ● Versioning documents (automatic versioning) ● Storing documents

	<ul style="list-style-type: none"> • Customizing applications for each State (radio buttons or drop downs) • Central database where all information is stored.
--	--

2.8 NEXUS/ VOLUNTARY DISCLOSURE HIGH-LEVEL BUSINESS PROCESS DIAGRAM



2.9 NEXUS/ VOLUNTARY DISCLOSURE BUSINESS PROCESS REQUIREMENTS

The Voluntary Disclosure Process is unique due to the fact that the taxpayer does not reveal their identity until the closing of the process. This would allow the MTC to incorporate items on the framework of the public website. Therefore, at this time, the Nexus Requirements will not be included in the Secure Communications Framework.

Data Types

The Nexus/ Voluntary Disclosure Process involve the following: application forms containing tax data, income data, and state requested information.

SR-04 Business Process to be put in place

- Roles Management
- Document Management

3.0 SECURE COMMUNICATIONS REQUIREMENTS

3.1 FRAMEWORK FUNCTIONAL REQUIREMENTS

3.1.1 Operational Requirements

SR-01	Users must be validated and authenticated in order to access and use the system.	
	Assumptions:	
		Users must adhere to the MTC user id policy
		MTC personnel will be responsible for assigning a username and password.
		Users must be authenticated in order to access and use the system
		Any system or application must enforce the user policy of renewing their passwords every 60 days
		Any system or application must enforce the user policy of a minimum of seven characters and contain alphanumeric characters and where allowed include special characters
		Any system or application must enforce the user policy of lock out after 3 unsuccessful attempts.
		Any system or application must support a User Hierarchy with administrators, users and super users. User account management will adhere to the MTC policy.
		Any system or application must block the ability of the user to store their password in any file program, command list, procedure, macro or script where it is susceptible to disclosure or use by anyone other than its owner.
	Accounts will be immediately disabled when the user's employment is terminated or the user transfers to a position where access is no longer required.	
SR-02	The Secure Communications Framework must comply with MTC Policies	
	Assumptions:	
		The policies will be the MTC Security Policy, MTC Acceptable Use Policy, and the MTC Confidentiality Policy. Please refer to Appendix A.
	The summary was drafted by Tim Blevins and will be finalized with the MTC and the Technology Committee	
SR-03	System Level Reporting Process	
	Assumptions:	
	To ensure security controls remain in place	

		Security Incident Reporting Process should be in place and documented
SR-04	Federal Tax Information Management	
	Assumptions:	
		All Federal Tax Information will be given to MTC through State channels. No federal tax information will be received by the taxpayer directly.
		The management of the Federal Tax Information will be in compliance with Draft Publication 1075: Tax Information Security Guidelines for Federal, State, and Local Agencies.
		Federal Tax Information should only be accessed by authorized personnel. The chain of custody must be recorded. Any system or application that utilizes Federal Tax Information must have the ability to track a user.
		Any system or application that stores the Federal Tax Information must be in a secure facility with controlled access. The servers must reside in a DMZ, and only applications that require the Federal Tax Information data will have access to that database.
SR-05	Disaster Recovery	
	Assumptions:	
		The MTC Secure Communications Framework will comply with the MTC Disaster Recovery policy.
		Any database that contains taxpayer confidential must have disaster recovery procedures.
SR-06	Non- taxpayer confidential data but requires security	
	Assumptions:	
		There will be a functionality evaluation for requests to be incorporated into the Secure Communications Framework.
		The Secure Communications Framework should be flexible enough to accommodate the business needs of the MTC.
		Litigation Request for an Expert Witness Database and a Legal Brief Database
		Nexus Voluntary Disclosure Application requires a framework where states and corporations are able to negotiate settlements anonymously while MTC facilitates.
SR-07	Data Disposal	
	Assumptions:	
		MTC will follow guidelines for the disposal of confidential data. For example, Confidential documents will be shredded, and systems will be thoroughly wiped and all data removed prior to disposal.

3.1.2 Physical Requirements

SR-08	Physical Access Control	
	Assumptions:	
		The system will be located in a restricted area where access is limited to authorized MTC personnel. Electronic security systems should be in place.
SR-09	Personnel	
	Assumptions:	
		Authorized personnel should be accessing the system via identification systems.
		Personnel will receive access according the principle of least privilege.
SR-10	Fire Suppression, Electronic Power Back-ups, and Environmental Controls	
	Assumptions:	
		UPS systems, Raised Floors, and climate control,
SR-11	Equipment	
	Assumptions:	
		Only MTC equipment or authorized state employees will have access.
		Employees accessing taxpayer confidential data must be in a secure location
SR-12	Alternative Worksite	
	Assumptions:	
		All alternative worksites should provide the same protections as the MTC location

3.1.3 Cyber Requirements

SR-13	MTC requires a secure channel to send documents to authorized state personnel	
	Assumptions:	
		The documents will be secured upon leaving the MTC and upon receipt at state designation.
		There must be proof that the transaction is performed or non-repudiation.
		There must be an audit trail for each transaction.
		The data must be encrypted during transport.

SR-14	MTC requires a secure channel to receive documents from authorized state personnel	
	Assumptions:	
		The documents will be secured upon leaving the state and upon receipt at MTC
		There must be proof that the transaction is performed or non-repudiation.
		There must be an audit trail for each transaction.
	The data must be encrypted during transport.	
SR-15	Roles must be defined and managed	
	Assumptions:	
		MTC personnel will manage roles and assignments. They will be responsible for the delegation process.
		A Roles and Responsibilities Process should be defined, for ex. Definition of User: permissions and responsibilities.
	A Security Administrator Role should be created for oversight of the security procedures for the Secure Communications Framework and the MTC website	
SR-16	Secure Location for Data Posting	
	Assumptions:	
		Utilizing a secure channel, MTC will provide a secure location for data to be viewed by those with appropriate permissions.
		Acceptable Data and File Formats should be agreed upon and the policy should be posted for users.
		Data Access must be restricted and no guest or anonymous accounts will be allowed.
	Access will only be allocated as necessary for project, job, or assignment	
SR-17	Database	
	Assumptions:	
		All access and modifications to database should be logged and tracked.
	Data should be backed up and tapes should be stored offsite for disaster recovery.	
SR-18	Network Security	
	Assumptions:	
	MTC Secure Communications Framework should be built on a secure Network for the LAN and WAN.	

		The following Network Security Measures will be included: Firewalls, Intrusion Detection Systems and Intrusion Prevention Systems, Virus Detection, Wireless Security, and Network LAN WAN Management and Security Procedures.
SR-19	Application and System Security	
	Assumptions:	
		Any Application built should to ensure that all security policies and measures are upheld.
		The systems should be built and “hardened” to comply with MTC Security Policy.
SR-20	Federal Tax Information Management	
	Assumptions:	
		All Federal Tax Information will be given to MTC through State channels. No federal tax information will be received by the taxpayer directly.
		The management of the Federal Tax Information will be in compliance with Draft Publication 1075: Tax Information Security Guidelines for Federal, State, and Local Agencies.
SR-21	Non- taxpayer confidential data but requires security	
	Assumptions:	
		There will be a functionality evaluation for requests to be incorporated into the Secure Communications Framework.
		Litigation Request for an Expert Witness Database and a Legal Brief Database will be considered for the Members Only section of the Public Website.
		Nexus Voluntary Disclosure Application will be considered for the Website.

4.0 REGULATIONS AND GUIDELINES DISCUSSION

MTC has always supported security as part of its culture. With the Secure Communications Plan and the management of taxpayer confidential data, the organization will have to comply with the following Regulations and Guidelines:

Computer Fraud and Abuse Act: This pertains to the protection of the data from unauthorized access and usage.

Carter Paperwork Reduction Act: This pertains to federal agencies information collection policies, the protection of that data, reporting procedures, and assessment of the paperwork burden.

Draft Publication 1075: Tax Information Security Guidelines for Federal, State, and Local Agencies: This pertains to guidelines for securely storing Taxpayer information, system controls and assessment, transmission of federal taxpayer information, and data warehouse concepts and security.

NIST Special Publication 800-26: Revision 1 Guide for Information Security Program Assessments and Systems Reporting Form: This pertains to the evaluation of security policy and procedures and on-going assessment of systems and programs.

5.0 SECURE COMMUNICATIONS SOLUTIONS

5.1.1 Introduction

Currently, the Multistate Tax Commission is forced to use non-electronic communications for most processes due to the lack of a secure communication framework. During the evaluation almost all communication was done via mail or fax. Users are also stripping tax payer confidential information from documents, and then sending them via email. This could create numerous security risks. The conclusion is to offer 2 secure communications solutions with varying security levels, functionality, flexibility, and set up requirements.

5.1.2 Option 1: Secure FTP

5.1.2.1 Overview

Secure FTP is an FTP client program which uses a graphical interface. It allows you to communicate with a remote FTP server to upload files and perform other functions. Users must log in to the system, upload the file they would like to transfer, and the transmissions are secured using SSL or SSH. SSL is implemented through the browser, encrypts the transmission in both directions, and ensures through password controlled access to the system that data can be securely transmitted in both directions. No tokens or special installation will be required at the users' browsers to ensure that the security is in place. This is the system that is widely accepted for internet security, and is most notable for its use in ecommerce websites (<https://>).

Most applications will provide logging and tracking. There are a wide range of vendors that offer Secure FTP services. IPswitch offers a basic package that is very low cost to Tumbleweed full solution that combines hardware and software for a full solution.

5.1.2.2 Pros and Cons

Pros

The Secure FTP solution would be very easy for set up. This is a low cost and low upfront set up solution.

Considering the existing infrastructure, there is an external DMZ already set up. A secure ftp server and database server could be quickly set up, and pending vendor selection, software could be assigned. With the launch of the MTC website, a user directory already exists, and future users could email requests and receive log-in credentials.

Cons

This solution would only satisfy the requirement to secure the data at the transmission level. It does not ensure that the data is secure once received by MTC. Database setup would be required for this security requirement. It also is not able to expand to some of the other business process requirements for the application.

5.1.3 Option 2: Secure Portal

5.1.3.1 Overview

This web portal would provide appropriate, controlled access for the various types of users to the applications. This portal will be the front end to the various MOSS sites that manage the files concerning a given single audit, and provide access for member states, MTC management, and the taxpayers for information relevant to them, and for which they are allowed access. The web portal functions would include:

- 1) For Auditors:
 - a. Timesheet submission
 - b. Status report submission
 - c. State audit issue tracking and resolution
 - d. Central repository (through WSS Project Sites) for current audit work products
 - e. Repository of current state templates
 - f. Access to audit tools or other applications
 - g. Central server for version control of the Auditor Desktop Application through the .Net Click Once deployment technology
- 2) For States:
 - a. Portal for making the final audit available securely for download to the states
 - b. State audit issue tracking and resolution
 - c. Mechanism for submitting audit candidate recommendations
- 3) For Taxpayers:
 - a. Mechanism for uploading information securely to auditor
 - b. Secure communications for downloading the preliminary and final audit
- 4) For MTC Management
 - a. Secure means for MTC supervisors to review the audit progress, and issue resolution for their audits
 - b. Secure means for the MTC Audit Director to review the status of all audits and State issue resolution
 - c. Timesheet reporting by auditor, audit, tax type, state, taxpayer, etc.
 - d. Secure mechanism for managing the annual taxpayer audit selection process, including receipt of recommendations, and the distribution of taxpayer documentation for review.
 - e. Single location for the management of state audit templates
 - f. Distribution of the latest Auditor Desktop Application updates
 - g. Version control and backup of all audits
 - h. Secure location for receiving and tracking revenue results from audits from the states.
 - i. Administrative functions to set up new audits, and manage the roles of the audit participants and the access the various stakeholders have to the audit system.

Secure Data Transmission – The application would implement Secure Socket Layer (SSL) as a means of providing security for the transmission of data between the various parties involved in the audit. SSL is particularly appropriate, in that it provides the high level of security needed in an environment where MTC will not control the external networks, computers or browsers through which the taxpayers, states, or others may need to access the system.

Access to data is controlled through a role-based system. Each user will be assigned a role, which will control his access to Audit Web Portal functions and individual audits. Within each individual audit, the auditor can easily control the release of audit work products (such as the release of the preliminary audit for taxpayer review), as the audit progresses.

5.1.3.2 Pros and Cons

Pros

The secure web portal is extremely scalable and flexible. The security is not limited to the transmission of the data. Through controls of the portal, views and access to portions of data could be controlled through the design of application and role based user management. This solution would be able to meet all of the secure communications requirement and accommodate the non-taxpayer confidential business needs

Cons

This solution requires an extensive requirements phase in order to design and set up the solution. Portal software is quite expensive, and hardware set up and configuration would be at least a one month process. The development of the portal would be a process that is very similar to the creation of the website. It requires a full development lifecycle, and the process timeline would be a minimum of 3months depending on the approved functions and phases of launch.

6.0 APPENDIX 1: POLICY AND PROCESS LISTS

6.1 POLICY AND PROCESS LISTS FOR MTC

Note: All responses below are taken from the Default Security Policy for the State of Kansas.

6.1.1 Personnel Security Policy:

Personnel Services

Working in conjunction with IT Management, Personnel Services' responsibilities include, but may not be limited to:

- ensuring that IT positions have job descriptions that accurately reflect appropriately segregated duties and responsibilities
- determining any necessary security clearances for individuals working with sensitive and/or confidential data
- conducting background checks as necessary for individuals in positions with sensitive job duties and responsibilities
- providing for appropriate division among several individuals for any highly secure functions
- establishing hiring, transfer, and termination procedures to promptly establish, modify, and close out security access
- documenting that all employees sign the Employee Consent Form for the Acceptable Use Policy and the Confidentiality Oath
- requiring that regularly scheduled vacations be taken
- promptly enforcing the Personal Conduct and Disciplinary Procedures for any significant security violations
- providing mandatory annual Security Awareness training for all employees and document attendance and maintain records.

6.1.2 User ID & Password Policy (including identification and authentication):

User Security

User Security addresses the ability to ensure that the user accessing data and systems is in fact who they say they are, present the necessary credentialing information for access, and that they have access only to those resources to which they are authorized. Functions that are involved include identification, authentication, authorization, non-repudiation, and audit.

Identification

The Agency must require that all users accessing protected information systems are properly identified. Each user must be required to provide some unique identification (User Id, token, biometric) to provide a claimed identity to the system. No guest or anonymous accounts will be allowed.

User Ids must:

- be unique and identify only one individual user
- not be shared and group user-ids should not be permitted, except where required by specific applications or computer platforms
- have their privileges terminated when they become inactive or dormant after a certain period of inactivity
- use a standard format developed by the Agency across all platforms to ensure uniformity
- only be issued after Security Administration receives a properly authorized request, indicating type of access desired
- be immediately disabled when the user's employment is terminated or the user transfers to a position where access is no longer required. The immediate supervisor or manager should initiate removal notification
- be suspended after 3 unsuccessful log on attempts.
-

Passwords must be:

- individually owned
- kept confidential and not shared with other users
- changed whenever disclosure has occurred or may have occurred, and changed at least every 60 days
- changed significantly (i.e., not a minor variation of the current password)
- a minimum of seven characters and contain alphanumeric characters and where allowed include special characters

Passwords must not be:

- repeated for at least six cycles of change or a year
- repeating sequences of letters or numbers (e.g. rrr, 123123)
- names of persons, places, or things that can be closely identified with the user (i.e., spouse, children or pet names)
- the same as the user id
- words that can be found in a dictionary
- displayed during the entry process
- written down and displayed in an obvious place
- the same for all systems the user accesses
- stored in any file program, command list, procedure, macro or script where it is susceptible to disclosure or use by anyone other than its owner.

The Agency CIO or senior IT Manager and the Security Officer or the Agency Head designee must approve all exceptions.

Vendor installed default passwords w must be changed immediately. If vendors require access to the system remotely for maintenance, they should be provided temporary passwords that are changed after they have concluded any maintenance.

Having and supplying the correct information authenticates an individual to the data processing system. Similarly, a computer, terminal, or other peripheral may be authenticated as an authorized device of a data processing system.

6.1.3 Authentication

The need for authentication is a response to the need to avoid or reduce the risk that the wrong person will access, use change, delete or otherwise improperly interact with valuable data or transactions

Authentication is the process and documentation required to validate a user's claim to who he/she is. Authentication can also be a process in which electronic devices validate who they are to one another. The strength of authentication can range from weak to strong. The selection of authentication strength should be based upon the level of risk consequence if security was breached

The Agency must require all users to be authenticated. Authentication should be based on something the individual knows (e.g. a password), something the individual possesses (e.g. a digital certificate, or smart card/smart token), or by something the individual is, (something which relies on measurable physical characteristics).

Systems must implement authentication functions that are consistent with the level of confidentiality or sensitivity of the information they contain and process. When considering authentication techniques, first determine if the confidentiality and/or criticality of the information processed by the system requires stronger authentication than passwords alone. If so, then consider smart cards, smart tokens, digital certificates or biometrics.

6.1.4 Authorization

Once identified and authenticated, Users must only have access to those resources to which they are authorized.

Authorization involves the determination of the proper level of access for all users for all systems, based on need to know, specific job responsibilities, and sensitivity of the data. The following points identify attributes of an effective authorization system:

- The authorities to read, write, modify, update, or delete information from automated files or databases should be established by the owner(s) of the information.
- Users shall be granted rights and privileges to available system resources only on a need-to-know, need-to-use basis. Users should be limited to the minimum rights and privileges to do their jobs.
- Individuals may be granted a specific combination of authorities.
- Data owners or their designees should review users' rights and privileges annually.
- Security administration should not require programmer intervention.
- Security administration activity should be recorded and reviewed and security violations should be detected and reported.
- There should not be any access available to programmers that is not provided through standard, approved connections. In other words, "backdoors" should not be permitted.
- Programmers responsible for development activities should not make changes to production application code without using the authorized change control procedures.
- Access rules or profiles should be established in a manner that restricts departmental employees from performing incompatible functions or functions beyond their responsibility and enforces a separation of duties.
- Procedures are enforced so that application programmers are prohibited from making unauthorized program changes.

6.1.5 Awareness & Training Policy:

The security administration function provides administration for user access to systems. These responsibilities include, but may not be limited to:

- authentication (add, change, delete) services to provide users with user ids and passwords
- authorization (add, change, delete) services to provide user access to applications
- generation and distribution of reports for monitoring access and potential security breaches
- management of the development and maintenance of Agency security policies and procedures deployment of mandatory annual Security Awareness training for all employees.

6.1.6 Incident Response and Reporting Policy:

Security Incident Reporting

There are several categories of information security incidents. Some examples are loss of service, human errors, computer fraud, viruses, network penetration, and loss of data or equipment. All suspected information security incidents must be reported as quickly as possible through the appropriate channels.

The responsibilities of the various parties are as follows:

- All employees, contractors and third party vendors should be required to immediately report suspected security breaches to their immediate supervisor.
- Employees, contractors and third party vendors should be advised that they should not, in any circumstances, attempt to prove a suspected weakness, without expressed prior authorization.
- Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents. Supervisors must notify the appropriate business area manager and the Agency Security Officer or designee
- Each Agency's Chief Information Officer, or senior IT Manager, will investigate, research, resolve, and document the event. If the event the Agency determines the event is of enough significance and seriousness, it shall be reported to the Kansas Information Technology Security Officer.

6.1.7 Maintenance Policy:

Revision Management

Revision management is a critical security ingredient in systems development, testing and maintenance. The following policies must be followed:

- Only one version of the application programs will ever reside in production libraries.
- The persons writing or maintaining code must not be the same person(s) who migrate code to production libraries.
- Only authorized personnel, with appropriate security permissions, should apply program changes, catalog and copy newly updated programs to production libraries.
- Once an application has been placed in production, all program changes must be approved by IS management to insure the changes have been authorized, tested and documented.
- The software change procedures shall include written notification to the appropriate departments of the change.
- Change Control procedures must ensure that the appropriate manager has authorized all moves between test and production environments in writing.
- Program development personnel shall access production data and production program files only to resolve emergencies. The appropriate management shall log all such accesses.
- All programs shall be installed into production from the source code. That is, the appropriate change control staff will recompile the programs into the production libraries.
- Software that is downloaded from the Internet shall not be used for processing confidential or sensitive information, until such software is thoroughly researched and tested to ensure it does not contain malicious code.

6.1.8 Configuration Management Policy:

System Security

System Security involves the analysis of the overall operating systems and software used to support the applications software. Whether the operating system is mainframe, server, or PC based, or a combination thereof, operating system technicians should:

- Ensure that research is done to identify security vulnerabilities.
- Maintain a log of investigations for these vulnerabilities for future reference.
- Maintain a system to become aware of, test and install vendor-supplied security upgrades and patches.
- Review and change vendor-supplied security parameters as required.
- Change shared system admin passwords when an employee with system administration responsibilities leaves the Agency.
- Utilize standard base configurations for operating systems on servers and workstations.
- “Harden” servers based on industry guidelines.
- Remove or disable any service not required.
- Test all upgrades or new releases of system software before deploying to production. Include analysis of any changes affecting security controls and training necessary to implement them.
- Acquire additional security software as needed to reside on the system to enable Agency to move from a reactive to a proactive environment.
- Install firewalls and monitor them.
- Install intrusion detection/prevention systems and monitor them for unauthorized access.
- Conduct periodic vulnerability scans and consider security audits by outside third parties to pinpoint the weaknesses of the system.

6.1.9 Acceptable Use Policy:

Acceptable Use Policy

The Agency must have an Acceptable Use Policy for Agency provided Information Technology Resources. All employees must be required to annually read it, and sign an Employee Consent Form indicating that they have read, understand and consent to the Agency’s Acceptable Use Policy. This form will be stored in the employee’s personnel file.

The Agency has issued an Acceptable Use Policy for Agency provided Information Technology Resources. These resources include, but are not necessarily limited to software, hardware, fax machines, pagers, cell phones, computer printers, E-mail, Internet, and voice mail.

Inappropriate use of the Agency's equipment may subject the employee to disciplinary action up to and including termination of employment.

The Acceptable Use Policy covers all forms of usage of these resources, whether used at work, at home, or in other locations. The Agency attempts to secure all computer resources used in the work environment and to restrict the access/entry of personnel to only authorized individuals.

6.1.10 Confidentiality Policy:

Confidentiality Provisions

If the Agency uses any type of confidential information (such as IRS data), the Agency must develop a Confidentiality Policy and an associated Confidentiality Oath. This Policy should cover all confidential information whether state or federal and enumerate the civil and criminal sanctions against unauthorized disclosure.

All employees must be required to read the Confidentiality Policy annually and sign the Confidentiality Oath, which will be stored in the employee's personnel file.

6.1.11 Security Assessment Policy:

The Agency IS management will annually update the State of Kansas Information Technology Security Self-Assessment in accordance with ITEC Policy 4310.

6.1.12 Contingency Planning:

Availability of Critical Data & Systems

The State of Kansas, Executive Branch Chief Information Technology Officer requires agencies to have a Business Continuation Plan that includes the procedures necessary to assure the continuation of vital State operations in the event of a disaster. Each division within the Agency must identify and prioritize its processes in its continuation plan.

The Business Continuation Plan must outline the internal policies and procedures that are to be employed should a disaster occur. Preparation of the recovery strategies for all time-sensitive processes must be coordinated with the Agency's Business Continuation Manager. In the event of a disaster all time-sensitive services, systems and applications must be restored and available on a priority basis to maintain vital Agency operations.

Time-sensitive applications include those systems whose loss or unavailability is unacceptable to the citizen's of Kansas. The loss or unavailability of support services provided to these applications may adversely affect the continuation of vital programs and services or the fiscal or legal integrity of the Agency operations.

6.1.13 Risk Assessment:

Risk Management

The principal goal of an organization's risk management process should be to protect the organization and its ability to perform their mission, not just its IT assets. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. The network will be continually expanding and updated, its components changed, and its software applications replaced or updated with newer versions. In addition, personnel changes will occur and security policies are likely to change over time. These changes mean that new risks will surface and risks previously mitigated may again become a concern. Thus, the risk management process is ongoing and evolving. (see also National Institute of Standards and Technology: Risk Management Guide for Information Technology Systems, Pub. 800-30)

The Agency will develop an inventory of critical information assets. Each division within the Agency must prioritize its applications in the application priority list in the Agency contingency plan. The Agency IS management will identify and analyze threats to the critical information assets to determine the likelihood of their occurrence and their potential to harm these assets. Security policies and procedures will be evaluated and documented to reduce these risks to acceptable levels. (see also Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments, CMU/SEI-2005-TN-032, Carnegie Mellon University, September 2005)

6.1.14 Access Control Policy:

The following practices must be adopted in order to maintain adequate physical security within the Agency offices:

Access control measures

- All servers and other sensitive pieces of hardware should be kept in locked rooms.
- All hub rooms, communications rooms for telecommunications and wiring closets must be secured and kept locked at all times, unless personnel are working in such rooms.
- Secure storage areas for laptop computers should be available within Agency offices.
- Laptop computers that are used outside the office and that contain confidential information should have some means of protecting the data, such as encryption or maintaining the data on removable disks.
- Whenever an employee leaves the Agency for other employment the immediate supervisor must obtain the employee's building passes and card keys. The supervisor must also notify Security Administration immediately upon an employee's separation.
- An Agency must have policies and procedures in place for locking doors after work hours.
- The home user of Agency equipment must ensure that unauthorized access to Agency resources is prevented.

Raised floor computer rooms must include the following control measures:

- Walls separating work areas on raised floors where the level of security is different on either side of the partition must extend and completely shut off the area between the raised floor and the permanent floor.
- An access card system will be used to control access to the room and will signal an alarm when unauthorized entry is attempted.
- Only persons whose work requires them to be in raised floor computer rooms on a day to day basis will be granted access cards to those areas.
- All visitors to computer room facilities must sign in on a log.
- Logs of all visitors to computer rooms will be maintained for a minimum of 1 year for audit purposes.
- Formal procedures must be established for the issuance and removal of card keys.
- Security Administration is responsible for processing requests for new cards, changes to existing cards and deletions of cards.

6.1.15 Audit Procedures:

Audit Trails

Automated records should be maintained to enable reconstruction and/or review of transactions performed on systems by users. Audit trails should be protected in such a way that a user can not change them. They should be reviewed regularly by individuals in a supervisory or security capacity, using automated tools where possible to review them.

Audit Trails for two other types of activities are also very important.

Security Administration Activities.

Access to security administration software must be restricted to personnel who have security administration duties. Audit trails must be maintained to provide accountability for all security administration activity. Software products used to administer security on all Agency systems must be able to record and report all security administration activity. Systems should also provide a means to recover current and historical information about security administration activities in the event of a system failure.

Security administration products and procedures must log all security violations. Resultant log files should be reviewed by security administrators and data owners to detect any unusual or inappropriate activity. In addition to checks against authorizations, particular attention should be paid to unusual times, frequency, and length of accesses, as well as irregularities that could indicate potential violations. Log data must be kept at minimum of 30 days.

The system must not disclose passwords through reporting functions.

Procedures must exist to maintain the integrity of access tables within security enforcement software.

Database and Other Logging.

Automated chronological or systematic records of changes to data are important in the reconstruction of previous versions of data in the event of corruption. These records are useful in establishing normal activity, identifying unusual activity, and in the assignment of responsibility for corrupted data.

A complete history of transactions will be maintained for each session involving access to confidential information to permit an audit of the system by tracing the activities of individuals through the system. The department's owner of data must determine how, where, and, the length of time that these transactions will be maintained.

In addition to system start-up and shutdown times, transaction histories should log the following information:

- update transactions
- date, time of activity
- user identification
- sign-on and sign-off activity and

- confidential display transactions.

DBA s' security actions should also be logged. Only designated personnel should have access to the transaction histories and to the results of any analyses.

Where confidential information involves the uses of Federal Tax information from the IRS, or any other data protected by Federal laws and regulations, appropriate audit trails must be maintained.

6.1.16 System & Information Integrity Policy:

System Integrity requires that hardware and/or software features will be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.