



TAX SHELTERED COMPENSATION, INC.

INFORMATION SECURITY AND CONFIDENTIALITY

REPORT ON CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS

**FOR THE PERIOD:
SEPTEMBER 1, 2008 – AUGUST 31, 2009**

TABLE OF CONTENTS

INTRODUCTION	1
SECTION I - INDEPENDENT SERVICE AUDITOR’S REPORT	2
SECTION II - DESCRIPTION OF CONTROLS PLACED IN OPERATION	4
COMPANY OVERVIEW	4
CONTROL PHILOSOPHY	4
SECTION III - CONTROL OBJECTIVES AND RELATED CONTROLS	5
CONTROL OBJECTIVE SUMMARY	5
ACCESS RIGHTS ADMINISTRATION AND AUTHENTICATION	7
NETWORK ACCESS.....	8
OPERATION SYSTEM AND APPLICATION ACCESS	9
REMOTE ACCESS.....	10
PHYSICAL SECURITY	11
BUSINESS CONTINUITY CONSIDERATIONS	12
OPERATIONAL CONSIDERATIONS	13

TABLE OF CONTENTS

SECTION IV - ADDITIONAL INFORMATION PROVIDED BY TSC	14
RISK, SENSITIVITY, AND CRITICALITY	14
ADMINISTRATIVE ACCESS CONTROL	17
SECURITY OF FACILITIES.....	21
ENCRYPTION.....	22
MALICIOUS CODE	22
ELECTRONIC AND PAPER-BASED MEDIA HANDLING	23
LOGGING AND DATA COLLECTION.....	24
SERVICE PROVIDER OVERSIGHT	24
BUSINESS CONTINUITY CONSIDERATIONS	24
OPERATIONS	25
CONTINUING EVALUATION AND ADJUSTMENT	27

INTRODUCTION

Tax Sheltered Compensation, Inc (hereinafter “TSC”), believes that it and each of its customers (hereinafter “Client”) is a repository of Non-Public Confidential Information (NPCI) and that each respective party has an affirmative and continuing obligation to protect the security and confidentiality of the NPCI it maintains as well as all NPCI it may gain access to through its business relationships.

This document is intended to provide TSC’s clients and their independent accountants with information about its control structure specific to protecting NPCI and selected operational controls. This report has been prepared taking into consideration the guidance contained in AICPA Statement on Auditing Standards No. 70, “Service Organizations” as amended.

There are four sections to this document. The first section includes a copy of the report provided by the independent accounting firm of Baune Dosen & Co LLP. The second section provides a general introduction describing the operating environment controls of TSC. The third section describes in greater detail the controls over the various types of functions and services performed by TSC. For each type of processing, control objectives have been identified by TSC management along with combinations of manual and automated controls that have been designed to achieve the control objectives. The fourth section contains additional information provided by TSC.



SECTION I – INDEPENDENT SERVICE AUDITOR’S REPORT

Board of Directors
Tax Sheltered Compensation, Inc.

We have examined the accompanying description of controls related to information security and confidentiality at Tax Sheltered Compensation, Inc. (TSC). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of the Company’s controls that may be relevant to a user organization’s internal control as it relates information security and confidentiality; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily and user organizations applied the controls contemplated in the design of the Company’s controls; and (3) such controls had been placed in operation as of August 31, 2009.

The control objectives were specified by the management of TSC. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of TSC’s controls, individually or in the aggregate.

In our opinion, the accompanying description of the aforementioned controls presents fairly, in all material respects, the relevant aspects of TSC's controls over information security and confidentiality that had been placed in operation as of August 31, 2009. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and user organizations applied the controls contemplated in the design of the Company's controls.

The description of controls of TSC is as of August 31, 2009, and any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at TSC is subject to inherent limitations and, accordingly, errors or fraud, may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes may alter the validity of such conclusions.

This report is intended solely for the information and use of the management of TSC, their clients and the independent auditors of its clients, and is not intended to be, and should not be, used by anyone other than these specified parties.

Baume Dosem & Co LLP

October 26, 2009
Minneapolis, Minnesota

SECTION II – DESCRIPTION OF CONTROLS PLACED IN OPERATION

COMPANY OVERVIEW

Founded in 1966, Tax Sheltered Compensation, Inc. (TSC) helps businesses provide successful retirement plans. TSC provides expert consulting, design and administration services for businesses throughout the United States.

To perform services, TSC receives information from plan sponsors, their CPA's and/or the financial company hired to invest the plan assets. TSC's clients include businesses and non-profit organizations that sponsor 401(k), Profit Sharing, Defined Benefit, Cash Balance, 403(b) and Money Purchase Pension plans for the benefit of its employees. The services offered to each client vary based upon a range of services offered to meet the specific needs of each client based on the type of plan design they have and the resources available to them.

CONTROL PHILOSOPHY

To assist in TSC's efforts to protect and secure the NPCI of it, its clients, and its client's customers, TSC has adopted an Information Security Plan to work in concert with TSC's information security and confidentiality methods and procedures. In addition, key operating methods and procedures are documented. This information is presented in Section IV of this report and further describes TSC's controls placed in operation.

SECTION III – CONTROL OBJECTIVES AND RELATED CONTROLS

CONTROL OBJECTIVE SUMMARY

- #1 ACCESS RIGHTS ADMINISTRATION AND AUTHENTICATION
All TSC employee system resource access is identified and restricted based upon the minimum required work to be performed. Verification of a TSC employee in the system is based on the presentation of unique credentials to that system.
- #2 NETWORK ACCESS
The network is sufficiently protected by current technology and is limited to only authorized personnel.
- #3 OPERATION SYSTEM AND APPLICATION ACCESS
All licensed software access is appropriately limited within the various network clients and servers, as well as stand-alone systems by the System Administrator.
- #4 REMOTE ACCESS
Access to TSC network through remote means is adequately controlled and limited to authorized personnel.
- #5 PHYSICAL SECURITY
Physical security controls are established to secure NPCI.

#6 BUSINESS CONTINUITY CONSIDERATIONS

A Business Continuity Plan is maintained to enable the business to operate in the event of a disaster.

#7 OPERATIONAL CONSIDERATIONS

Client deliverables (documents, amendments, tax forms, etc.) are complete, accurate and timely.

The following section provides a matrix which individually lists the control objectives provided by TSC as described throughout this report. For each control objective, the left side of the matrix contains an indication of policies and procedures, which are designed to provide reasonable assurance that the stated control objective is met. The right side of the matrix describes tests of operating effectiveness and the results of those tests. The description of processing and control policies and procedures were prepared by TSC. The tests of operating effectiveness were prepared by Baune Dosen & Co LLP. The tests apply only to the stated control policies and procedures. They may not address all aspects of the processing activities described.

ACCESS RIGHTS ADMINISTRATION AND AUTHENTICATION

CONTROL OBJECTIVE 1: All TSC employee system resource access is identified and restricted based upon the minimum required work to be performed. Verification of a TSC employee in the system is based on the presentation of unique credentials to that system.

	DESCRIPTION OF CONTROL
1.1	A unique user ID is assigned to all new employees along with a minimum password length based on settings established in Active Directory Group Policy.
1.2	Passwords must be seven or more characters in length.

NETWORK ACCESS

CONTROL OBJECTIVE 2: The network is sufficiently protected by current technology and is limited to only authorized personnel.

	DESCRIPTION OF CONTROL
2.1	TSC has a Sonicwall firewall to protect applications and data.
2.2	Virus protection is installed on both servers and workstations. Virus signature updates are systematically pushed down to all workstations as updates are identified.
2.3	If a virus has been detected a message will appear on a user's computer.

OPERATION SYSTEM AND APPLICATION ACCESS

CONTROL OBJECTIVE 3: All licensed software access is appropriately limited within the various network clients and servers, as well as stand-alone systems by the System Administrator.

	DESCRIPTION OF CONTROL
3.1	Access to the TSC network and applications require that a user authenticate by entering in their network user ID and a confidential password.
3.2	After five invalid access attempts, the user ID is locked for a duration of 30 minutes.

REMOTE ACCESS

CONTROL OBJECTIVE 4: Access to TSC network through remote means is adequately controlled and limited to authorized personnel.

	DESCRIPTION OF CONTROL
4.1	Remote Access to TSC's network must be added to an employee's user profile by a System Administrator.
4.2	All remote contact with the TSC network is encrypted via a VPN connection.
4.3	Company issued cell phones with company email access can be remotely wiped clean immediately upon knowledge of the cell phone being lost or stolen.

PHYSICAL SECURITY

CONTROL OBJECTIVE 5: Physical security controls are established to secure NPCI.

	DESCRIPTION OF CONTROL
5.1	The side entrance of the office is locked with a keypad combination that only employees can use to enter. This entrance is always locked.
5.2	During business hours, 8:00 am to 5:00 pm, Monday to Friday, a receptionist is situated in the lobby.
5.3	The network equipment is located in a specific room, segregated from main office traffic. The room is secured by a key lock when the Network Administrator's office is not in use.
5.4	File servers are configured in freestanding rack mounted cabinets in the server room.
5.5	A fireproof cabinet is used to hold computer media.
5.6	UPS units are installed to protect the file servers and telecommunications equipment from power surges.
5.7	Environmental controls are used to protect the network equipment with an air conditioning vent in the warm months and exhaust fan during the cold months when heat is running in the building.
5.8	It is Company policy that company issued laptops taken outside of the office and left unattended in a vehicle be locked in the trunk and always maintained out-of-sight. If kept in a hotel room, they are appropriately secured. Laptop cable locks are used whenever possible.
5.9	It is Company policy that sensitive client data is not stored on the c: drive of a company issued laptop when it is taken outside of the office. Only the network system administrator may have such data for the purpose of project work and development.
5.10	Paper-based information received from clients is retained in the client hard-copy folders. All hard-copy information is electronically scanned into our system one year after the valuation has been completed. After being scanned, the hard-copies are kept in secure locked bins until shredded on site by a company contracted to perform this service.
5.11	Electronic-based information received from clients is retained in the client electronic folders.

BUSINESS CONTINUITY CONSIDERATIONS

CONTROL OBJECTIVE 6: A Business Continuity Plan is maintained to enable the business to operate in the event of a disaster.

	DESCRIPTION OF CONTROL
6.1	A Business Continuity Plan is in place to ensure the availability of services should a disastrous event interrupt service. The plan contains procedures for the recovery of the operating system and critical business applications.
6.2	At a minimum, back up retention is four weeks.
6.3	Media is properly labeled.
6.4	A copy of a full back-up is sent to off-site storage on a weekly basis.
6.5	The Business Continuity Plan is documented and updated to reflect the changing environment. The plan is updated as changes occur.
6.6	Back-up data is restored on a monthly basis to ensure that back-ups are running correctly.

OPERATIONAL CONSIDERATIONS

CONTROL OBJECTIVE 7: Client deliverables (documents, amendments, tax forms, etc.) are complete, accurate and timely.

	DESCRIPTION OF CONTROL
7.1	Prior to the last day of the plan year, TSC sends a Year End Request Package (YERP) to each client requesting the information necessary for TSC to perform the services outlined in our service agreement with the client.
7.2	If a client has not provided TSC with the information needed to complete the Average Deferral Percentage (ADP) testing within 1 month of the correction deadline, a follow-up email is sent reminding the client to forward the information. If the information has not been received 2 weeks before the correction deadline, a follow up phone call is made requesting the information.
7.3	For those clients that did not provide information prior to the testing deadline, additional follow up requests are sent prior to the un-extended and extended due dates for the Form 5500 filing.
7.4	A manual tracking checklist is prepared each year for each client to monitor the preparation and review of each item prepared. The preparer and reviewer each initial and date when steps are completed.
7.5	Each TSC Retirement Plan Administrator updates the work-in-process database for their assigned block of clients on at least a monthly basis.
7.6	Each TSC Retirement Plan Administrator and respective team managers/supervisors monitor key dates on at least a monthly basis.
7.7	The Vice President of Operations reviews key dates on a periodic basis.
7.8	Contributions and loan repayments recorded in the plan's investment statements are reconciled to the information provided to TSC in the YERP.

SECTION IV– ADDITIONAL INFORMATION PROVIDED BY TSC

TSC believes that it and each of its customers (hereinafter “Client”) is a repository of Non-Public Confidential Information (NPCI) and that each respective party has an affirmative and continuing obligation to protect the security and confidentiality of the NPCI it maintains as well as all NPCI it may gain access to through its business relationships.

The definition of NPCI is all non-public information received by TSC or Client in any form (written, electronic, or otherwise), either directly from the other party or from another source on behalf of the other party that relates to, or is identified with any Consumer, individual or business entity. NPCI shall include, but not be limited to:

1. All internal business, financial, operational, and technological data pertaining to TSC, Client, and their Representatives;
2. All internal data, general information, personally identifiable financial information, and/or records pertaining to any client, financial advisors or funding company platforms; and
3. Any information that is:
 - a. Not publicly available or
 - b. Derived in whole or in part from information that is not publicly available.

I. RISK, SENSITIVITY, AND CRITICALITY

To assist in TSC's efforts to protect and secure the NPCI of it, its clients, and its client's customers, TSC has adopted this IS Plan to work in concert with TSC's security methods and procedures. This Plan generally outlines TSC safeguards to protect NPCI but it does not detail the precise methods, standards and procedures used by TSC. Doing so would provide a tool that external parties might use in an effort to breach TSC's security measures. Therefore precise details regarding TSC's security methods, standards and procedures are provided in a confidential document to the firm that audits TSC and issues SAS 70 reports regarding TSC's adherence to its stated standards.

A. SECURITY GOALS

The general procedures and safeguards that TSC has adopted to achieve its security goals are:

1. Ensure the security and confidentiality of NPCI in TSC's possession.
2. Protect against any anticipated threats or hazards to the security or integrity of NPCI.
3. Protect against unauthorized access to or use of NPCI. The compromise of which could result in substantial harm to TSC, TSC's Client, and other third parties.
4. Identify and assess risks that may threaten NPCI.

B. IDENTIFIED SECURITY RISKS

TSC recognizes that it is not possible to make a definitive list of security risks to NPCI. TSC has recognized the following internal and external risks including, but not limited to:

1. Unauthorized access to NPCI by an unauthorized individual;
2. Compromised computer system security as a result of system access by unauthorized personnel.
3. The physical or electronic interception or destruction of NPCI during transit;
4. Loss of NPCI and or computer systems that contain NPCI due to a natural disaster;
5. Accidental or deliberate errors introduced into a computer system that contains NPCI;
6. Accidental or deliberate corruption of physical or electronic versions of NPCI;

7. Misuse of NPCI by TSC employees and/or representatives;
8. Requests for NPCI by unauthorized personnel;
9. Compromise of TSC's physical security that results in the unauthorized access of NPCI;
10. Unauthorized transfer of NPCI by or to a vendor.

C. SECURITY BREACH NOTIFICATION

In the event of a Security Breach, TSC will follow the procedures presented herein to provide notification to those Clients whose NPCI is reasonably believed to have been compromised. Notification will occur without unreasonable delay, except when:

1. A law enforcement agency has determined that notification will impede a criminal investigation. In such instances, Client notification will occur as soon as the law enforcement agency determines that such notifications will not compromise its investigation.
2. A reasonable delay is felt necessary in order to ascertain the scope of the breach and to restore the integrity of the compromised system.

TSC may determine the language to be used in the notification, which may be distributed in either a written, hard copy notice or by e-mail, in reference to the specifics of the security breach committed. If sufficient contact information is not available for a hard copy or e-mail notice, a telephone call may be used to provide prompt notification to Client.

D. INFORMATION SECURITY TEAM

Certain members of management will meet on an as-needed basis, but not less than once each year, to conduct a review of current security procedures and policies. This will be done to help determine if security adjustments and/or additional employee training are required. The team has the authority to respond to a security breach and is responsible for:

1. Assessing TSC's risks associated with NPCI;
2. Preparing cost comparisons for varying security approaches appropriate to TSC's environment;
3. Creating standards that guide managers and employees in implementing TSC's security methods and procedures;
4. Making certain that the employees in the various work units, departments and divisions in TSC abide by procedures and policies;
5. Maintaining comprehensive lists outlining:
 - a) All NPCI repositories at TSC
 - b) TSC hardware assets
 - c) TSC software assets
 - d) TSC network connections; and
 - e) TSC telephone and facsimile connections.

II. ADMINISTRATIVE ACCESS CONTROL

Administrative access controls have been established to restrict access to all TSC systems and system resources that house NPCI. Access to TSC systems that house NPCI is provided only to those employees who need access to such system(s) to complete their assigned work. This section outlines various administrative controls including, but not limited to, access rights administration and authentication protocols as they pertain to computer networks, operating systems, applications, via local and remote access. To help minimize the risk of unauthorized access, the following precautions have been instituted:

1. System Administrators who have controlling access to TSC's computer systems are appointed by the Information Security Team.
2. The access rights of each employee are configured at the proper level pertaining to the employee's position in the company.
3. All preconfigured "guest accounts" incorporated into hardware and software are disabled.
4. Mechanisms are in place to record when there are repeated failed attempts to gain access.
5. All employees are made aware of the serious consequences that may result from security breaches and their individual responsibilities to help prevent breaches.

System Administrators are provided full system access to perform essential system administration functions critical to the continued operation of TSC including, but not limited to: i) establishing User ID's; ii) maintaining authorization levels for all accounts; iii) terminating an employee's session; iv) correcting problems; v) and other broadly-defined system privileges. The number of System Administrators accounts is to be kept to the absolute minimum number necessary for TSC to have appropriate and satisfactory System Administrator coverage at all times. It specifically restricts the granting of System Administrator rights to only those employees whose job duties require them.

System Administrators administer the access rights for all employees. A user's access to system resources is restricted to the level of access required for that individual to perform his/her required work.

A. AUTHENTICATION PROCEDURES

Authentication involves the verification of a user's identity prior to providing access to computer resources. It is based on the user entering a unique username and password into the computer system to gain access to that system.

Upon request from a TSC manager to grant initial system access, a System Administrator will assign the employee to an existing access class. The employee is then given a registered and unique “User Name” that identifies that employee in the computer system and a password. The password must conform to various pre-established criteria that make it a password that is difficult to crack. The user has the option to periodically change his or her password throughout their term of employment.

To mitigate Authentication related risks, TSC has adopted the following requirements:

1. Employee passwords are required to be a minimum seven characters long.
2. The password authentication system is protected by an encryption algorithm when a privileged user logs into the network remotely.
3. Lockout mechanisms are currently in place to lockout access to the User ID after five failed attempts.
4. All messages regarding failed log-ins are non-descriptive in nature.
5. If a server session is inactive for longer than fifteen minutes, a screen blanking mechanism is activated. Prior to resuming activity, the System Administrator must re-authenticate before any action can take place.

B. NETWORK SECURITY

The Network System Administrator, one additional System Administrator and a third party contractor are authorized to add, remove, or replace network components. They are also charged with making certain all network and client devices, including their respective software, are appropriately maintained and managed.

To adequately secure access to TSC’s systems and NPCI, a variety of control mechanisms have been established including router and firewall technology. The network controls that distinguish security domains include access control software permissions, firewalls, remote access servers, and Virtual Private Networks (VPNs). To help identify and administer all of these access control points, a network diagram is continually updated to reflect any and all changes in the system’s topography.

Information regarding the firewall is deemed sensitive and is included in TSC's firewall standards. Those standards establish the rules for traffic coming into and going out of the TSC computer network and designate how the firewall will be managed. Areas covered by TSC's firewall standards include, but are not limited to:

1. Firewall topology and architecture;
2. Types of firewalls being utilized;
3. Monitoring firewall traffic when/if applicable;
4. Permissible traffic;
5. Firewall Updating;
6. Protocols and applications permitted based upon port filtering.

All administrative access to the DNS Hosts, routers, and switches are limited to only System Administrators. Remote administration must be done using encrypted communication and password authentication. To further secure any transmissions through the firewall, it has been configured to accept Network Address Translation and Virtual Private Network gateways.

Additional measures adopted by TSC to control access to the system software within the various network clients and servers or via stand-alone systems include:

1. Restricted access to sensitive or critical system resources.
2. Restricting user and program access to sensitive system resources including files, programs, or processes.
3. Update operating systems with security patches and using appropriate change control mechanisms.

C. REMOTE ACCESS

System Administrators and the pre-authorized staff are the only employees eligible to access TSC's network remotely. TSC uses Virtual Private Network (VPN) as the method of accessing TSC's network remotely. All remote users are to adhere to TSC's Remote Access Policy. The activity of remote session is logged and reviewed as deemed necessary.

III. SECURITY OF FACILITIES

TSC maintains locked, access controlled office space.

A risk assessment has been performed relative to various external physical risks such as: fire, water, smoke, theft, destruction (accidental or by design), static electricity, dust, and power surges. To mitigate these and other physical risks, TSC has adopted various standards and procedures.

Key elements of TSC's facilities security include, but are not limited to:

1. Access to the building is limited to two entrances. They are the employee entrance and the visitor entrance.
2. The employee entrance is kept locked 24 hours a day with a code required for entrance.
3. The visitor entrance is kept locked during non-business hours. A receptionist monitors access during business hours.
4. The building is equipped with a variety of motion, fire, smoke, heat and glass break detectors. During non-business hours, an offsite security firm monitors these building security systems. Fire extinguishers with contents matched to the area of deployment have been placed throughout the building. They are inspected, serviced, and recharged by a licensed fire extinguisher company.

A. INFORMATION TECHNOLOGY DEPARTMENT SECURITY

The Information Technology (IT) department houses TSC's physical network controls and the backups to the entire system.

The IT department has one access point and is kept locked unless if authorized personnel are in this office. A fireproof cabinet is used to hold installation and system back up media. System backups are created nightly and are kept for a minimum of a four-week period. Access to this area is controlled solely by the CEO of the company and is granted only to those individuals who require the access to conduct business.

IV. ENCRYPTION

TSC uses encryption protocols a) when communications must be secured; b) for authentication processes; c) for the transmission of sensitive information; d) to secure applications and remote access communications.

V. MALICIOUS CODE

TSC defines malicious code as any program that acts in unexpected and potentially damaging ways. Since malicious code is highly dynamic, has many mobile connection possibilities, and does not specifically have to be targeted at TSC, it maintains a high-risk potential. To reduce risk and protect TSC systems from malicious code TSC has established the following procedures including, but not limited to:

1. Use of anti-virus products, which use both signature and heuristic methods of detection and identification, on clients and servers;
2. Training system users not to open unexpected messages or executable files.
3. Training system users on what to do if they see an on screen alert that a virus has been detected.
4. Use of e-mail filters helps prevent the receipt of executable files.

VI. ELECTRONIC AND PAPER-BASED MEDIA HANDLING

NPCI is frequently contained on media such as paper documents, reports, back-up tapes, optical storage, test data, and system documentation. To maintain the security of NPCI requires that the media be secured. TSC considers all media to be equally sensitive and therefore, protects it all with equal diligence. Media handling and security is addressed in the following manner:

A. HANDLING AND STORAGE

All short-term storage of original media and media being worked on is kept on site at TSC until it is returned to the Client, archived or destroyed. All NPCI in long term storage is packed, labeled, and arranged in a specific manner to reduce the risk of loss and destruction.

B. DISPOSAL

1. PAPER BASED NPCI: To preclude the accidental inclusion of NPCI information in the regular trash, TSC employees are prohibited from discarding any paper, which contain NPCI, into regular trash bins. NPCI paper-based media must be placed into designated destruction bins that are emptied as they fill. Once a sufficient amount of paper-based media has accrued, a designated employee will make certain it is delivered to a designated media-disposal company. The media will then be destroyed in such a manner that it cannot be reasonably compromised or re-claimed.
2. ELECTRONIC-BASED NPCI: Since residual data frequently remains on electronic media even after erasure, all electronic-based media has specific disposal requirements. When possible, electronic media (i.e., CD's, disks, etc.) is destroyed. Otherwise, to destroy the electronic media, the data areas are overwritten by a System Administrator.

C. TRANSIT

TSC is not responsible for the security of any physically transported NPCI a Client transports to TSC until the NPCI is received by TSC. The receipt of the NPCI is logged. If the NPCI is damaged in transit, or missing, when compared to TSC's expectation, the applicable Client is contacted.

VII. LOGGING AND DATA COLLECTION

TSC has taken steps to ensure that sufficient data is collected to identify security incidents. TSC logs the following data:

1. Operating System Access.
2. Remote Access.

VIII. SERVICE PROVIDER OVERSIGHT

TSC rarely contracts for services outside of the company that require access to NPCI. However; should it be necessary to enter into an agreement with an outside services provider, that provider will be required to: a) implement appropriate security controls to comply with TSC's Information Security Plan; or b) provide TSC a copy of the provider's SAS 70 Information Security Plan with proof of audit.

IX. BUSINESS CONTINUITY CONSIDERATIONS

Events that could trigger the implementation of TSC's Business Continuity Plan would likely have significant security considerations. Therefore, TSC's Business Continuity Plan addresses the risk mitigation that would be necessary to protect TSC and the Client in the event the continuity plan must be implemented. Risk mitigation procedures have been established to cover a variety of contingencies including, but not limited, to the following:

1. TSC's office must be evacuated.
2. There is an equipment malfunction regarding computers or security systems.
3. Data or original media is corrupted, destroyed, and/or lost.

X. OPERATIONS

TSC employees prepare plan documents, amendments, Summary Plan Descriptions, annual valuations, discrimination testing, 5500s, 5558s on a complete, accurate and timely basis so that execution can occur in a timely manner.

In addition, TSC prepares a newsletter that is emailed quarterly to all of our clients. The purpose of the newsletter is to keep our clients abreast of changes in retirement plan legislation and to provide informative data as it relates to our client's day-to-day administrative plan duties.

For applicable clients, quarterly participant statements are prepared by TSC. When requested by the client, TSC will calculate the employer contribution allocation pursuant to the terms of the plan document. If an employer contribution is required (safe harbor or top heavy), TSC will calculate the allocation and advise the client accordingly.

TSC maintains policies and procedures to ensure that employees prepare complete and accurate information for clients on a timely basis. They consist of the following:

1. Prior to the last day of the plan year, TSC sends a Year End Request Package (YERP) to each client requesting the information necessary for TSC to perform the services outlined in our service agreement with the client. The YERP provides specific instructions for clients to provide the necessary information and outlines testing deadlines applicable to each client.
2. If a client has not provided TSC with the information needed to complete the Average Deferral Percentage (ADP) testing within 1 month of the correction deadline, a follow-up email is sent reminding the client to forward the information. If the information has not been received 2 weeks before the correction deadline, a follow up phone call is made requesting the information.

3. Once the ADP test has been completed, prior to the correction deadline for failed ADP tests an email is sent to the client advising them of the test results or a hard copy of the test results is included with the valuation reports mailed to the client.
4. In the event that late deposits of employee contributions are indicated, TSC will calculate lost earnings pursuant to the corrective measure chosen by the client. If the client chooses the VFCP process, all forms and instructions are prepared and forwarded to the client.
5. When the valuation and Form 5500 have been completed, TSC will forward a hard copy of the reports to the client with clear instructions on the action items that the client must complete. Also included in the correspondence is an explanation for any compliance issues identified during the valuation process.
6. All documentation for loans and distributions processed through TSC is retained in the TSC client files.
7. Contributions and loan repayments recorded in the plan's investment statements are reconciled to the information provided to TSC in the YERP.

TSC employees are required to communicate on a timely basis by performing the following:

1. Each TSC employee must respond to a client phone or e-mail inquiry directed to them within 24 hours.
2. All TSC employees that will be out of the office for a full business day are required to have an out-of-office message and voicemail message advising callers that they are out of the office and to contact another member of the team for immediate assistance.
3. If a plan is identified as falling out of compliance for any reason, clear communication regarding corrective action is provided to the client.

TSC employees track the status of each client's job to be completed by performing the following:

1. TSC maintains a database of current clients that tracks key dates for necessary workflow. Internally this database is referred to as Work-in-Process (WIP) reporting. Updating of the WIP database is performed by each TSC Retirement Plan Administrator for their assigned block of clients on at least a monthly basis. Monitoring of key WIP dates is performed by each TSC Retirement Plan Administrator and by each respective team manager/supervisor on at least a monthly basis. A third review of key WIP dates is performed by the VP of Operations on a periodic basis.
2. TSC requires each applicable client to provide by a specified date the information necessary to ensure TSC can timely complete the average ADP test. TSC maintains a separate tracking list for each client subject to the ADP test. Internally this tracking list is referred to as ADP Test Report. Updating of the ADP Test Report is performed by each TSC Retirement Plan Administrator for their assigned block of clients. Monitoring of ADP Test Report is performed by each TSC Retirement Plan Administrator and by each respective team manager/supervisor.
3. Client requests for Plan Document changes are input into the TSC database and monitored by our legal department to ensure timely completion.
4. For those clients that did not provide information prior to the testing deadline, additional follow up requests are sent prior to the un-extended and extended due dates for the Form 5500 filing.

XI. CONTINUING EVALUATION AND ADJUSTMENT

The Information Security Plan and any policies it references is subject to periodic review and adjustment. The most frequent of these reviews will occur within the TSC Information Technology department, where constantly changing technology and risks mandate that standards and procedures evolve to be effective. Continued administration of the development, implementation and maintenance of the program will be the responsibility of the Information Security Team which will assign specific responsibility for TSC information technologies implementation and administration as appropriate. The Information Security Team will review the standards set forth in the Plan and all associated policies, recommending updates and revisions to reflect changes in technology, the sensitivity of NPCI and internal/external threats to information security.