



Attorneys' Title Insurance Fund, Inc.

Information Services Policies and Procedures

Table of Contents

Note: The Policies and Procedures may contain multiple pages. Please refer to the page numbers to ensue you review the entire document.

1 Production

- 1 A – Conditional Production Acceptance Waiver
- 1 B – Production Change Policy
- 1 C – Production Uptime
- 1 D – On-Call Compensation
- 1 E – Production Problem Management Process
- 1 F – Production Problem Analysis Report Process

2 Personal Computing

- 2 A – Computer Hardware and Software Standards
- 2 B – Software Inventory Policy
- 2 C – Standardized Desktop Policy
- 2 D – Reproduction of PC Software
- 2 E – Computer Acceptable Use Policy
- 2 F – PC Inventory
- 2G – Remote Access Policy

3 Security

- 3 A – Employee Network Computer Password Policy
- 3 B – Computer Audit Policy
- 3 C – User Account Creation and Deletion Policy
- 3 D – Software Audit / Inventory Policy

4 Project Management

- 4 A – Project Change Management Process
- 4 B – Methodology

5 General

- 5A – Email Usage Guidelines
- 5B – How to Share Email Inboxes
- 5C – Internet Usage Policy
- 5D – Internet Web Content Policy
- 5E – Telephone Usage Policy
- 5F – Purchasing Information Technology

6 Applications

- 6A – Application Data Ownership Policy



Attorneys' Title Insurance Fund, Inc.
Policies and Procedures

Subject: Conditional Production Acceptance Waiver	Effective Date: 03/07/05
---------------------------------------------------	--------------------------

Authorized by: J. Calabrese

Title: SVP, Information Services

New/Revised: Revision 1

Purpose: To identify, approve and resolve production implementations that are granted with exceptions. The purpose of the Conditional Production Acceptance Waiver is to identify and communicate all changes to the production environment that are granted on a temporary basis; to identify who is responsible to remediate the exception(s) and provide a proposed date the exception(s) will be resolved. The document formalizes the waiver and provides a method for the Production Services Senior Manager to review and determine disposition.

Policy: It is a policy of The Fund to have all aspects of project production implementation completed before the project can be officially closed. Project implementations that are granted based on a conditional waiver, must follow the process / procedures stated herein. Once this process is completed, the project is eligible for closeout.

Procedures

1. A Conditional Production Acceptance Waiver must be completed by the Project Lead or Product Manager when approval to proceed with a production implementation is requested with exceptions.
2. The form must clearly define the exception(s), the reason for the exception, the work-around, the impact to internal or external customers, provide a proposed date the exception(s) will be resolved, and identify the responsible department(s) who will resolve the exception(s).
3. The form must be signed by the Project Lead, Product Manager, Project Sponsor, User Representative, Test Team and the IS Senior Manager who is responsible for correcting the exception.
4. The completed form must be sent to the Production Services (PS) Senior Manager for approval.
5. The information should be discussed at the project's "Go No-Go Meeting".
6. The PS Senior Manager will work with the appropriate management team to develop a plan to address the outstanding items.
7. The PS Senior Manager will then be accountable for ensuring these are resolved within the agreed upon time frame.

Request for Waiver

Requestor:	IR / SR Number:
Project:	Date:
Exception Type:	
Requirement <input type="checkbox"/> Test <input type="checkbox"/> Hardware <input type="checkbox"/> Other _____	
Waiver Type:	
Defer <input type="checkbox"/> Postpone <input type="checkbox"/> Other <input type="checkbox"/> _____	
Describe the Waiver:	Expected Resolution Date:
Reason for Waiver:	
Availability of Work Around:	
Impact to External Customers:	
Impact to Internal Customers	
Department or Team Responsible for Remediation:	

Sponsor	Signature	Date
Project Lead	Signature	Date
Product Manager	Signature	Date
Test Team	Signature	Date
User Representative	Signature	Date
Production Services	Signature	Date
IS Senior Manager (Correcting waiver)	Signature	Date



Attorneys' Title Insurance Fund, Inc.
POLICIES/PROCEDURES

Subject: Production Change Policy	Effective Date: 09/12/01
-----------------------------------	--------------------------

Authorized by: J. Calabrese Title: SVP, Information Services New/Revised:

Policy: The Production Systems Change Policy is in place to protect our users from disruption to their business processes, and the production environment from disruption and damage.

Procedure: The procedures defined herein are implemented in support of the policy.

- A. Changes will be implemented twice a week to be effective on either Wednesday or Friday mornings. **Only non-mainframe type changes are permitted on Wednesday.** Exceptions will be granted for Weekend implementations based on degree of changes and potential customer impact.
- B. All changes must be on a System Change Document (SCD).
- C. The SCD must include all signatures required by the Production System Change signature matrix. The signature of the Manager or Supervisor signifies that they have reviewed the Change Form and the User Signoff for accuracy and thoroughness. If the SCD is modified in any way, including implementation dates, signatures must be obtained once again prior to resubmitting.
- D. All changes must indicate a Backout Procedure to be followed if problems occur. Backout Procedures must include a detailed step-by-step task list with timeframes that will return the system back to its original production state. If the backout plan presented encompasses a timeframe including normal production hours, the plan must be approved by the Production Operations Manager.
- E. If a problem occurs during initial production testing, the programmer and user will have until 7:00 AM to identify and solve the problem. If the problem resolution takes us beyond our normal level of service to our customers, the change will be backed out. All changes requiring backout should be completed by 7:30. Changes to other platforms must be backed out 30 minutes prior to the scheduled production time. Backout procedures and timeframes must allow for testing after the backout is completed. In the event of a backout, the change must then re-enter the normal change process before any further attempts to implement into production.
- F. The Computer Operations Supervisor will ensure that the requests for changes to the online and client server environments, as well as network and hardware changes, are performed in the time frame after online shutdown and prior to the startup of the next business day.

- G. Computer Operations will ensure that the online production environment is up and available for the initial testing of changes by 6:00 A.M. Testing is coordinated by the Information Services Test Team and performed by the Test Team and designated users. Testing will include executing all changed modules and any other transactions or systems that interface with the changed modules.
- H. Requests for executing changes to the batch environment will be performed any time after the current night's processing is completed and prior to the next day's batch processing. For batch changes, the designated person(s) must be on call when the new modules are executed.
- I. The functional group implementing a change is responsible for ensuring that a brief synopsis of both successful and unsuccessful changes is submitted to Test Team via email immediately following the implementation. In the event the change is postponed, cancelled, or there is a change in the schedule, the change must re-enter the normal process. The Computer Operations Supervisor must be notified immediately upon discovering that plans have been altered.
- J. The Help Desk Manager will provide a report of all discrepancies resulting from changes to the Information Services Division Direct Reports.
- K. All changes for the week will be submitted to the Change Bin by Noon on Mondays with all signatures and a soft copy put on the J:/Shared drive under IS Change/Pre-Approved. The approval process will take place on Tuesdays and moved to Approval for all to review that week. In the event that a holiday falls on a Monday, the process will be pushed back one day.

For the file name, use your network sign on id, plus the date you wrote the change. (For example, **jfric 09-14-01.doc**)

Exceptions

- A. Changes to address critical or high incident reports (IR) are changes that are required to allow the user(s) to continue productive work.

Without these changes, it is understood that the user(s) cannot function within the transaction, program, or system affected.

- B. Changes resulting from critical or high IRs are to be completed and tested by the appropriate technical personnel. During normal business hours, the Help Desk must be notified of all changes. The Help Desk will then notify the Computer Operations Supervisor and any other appropriate personnel. Outside of normal business hours, an IR will be generated for documentation and notification. Critical and high software changes must be followed by the appropriate change document within one business day of the change being completed. This documentation should be placed in the designated "Change Bin." Exceptions regarding the required documentation may be deemed appropriate by the Production Operations Manager.

Note: For business reasons, there may be other exceptions as determined by the Production Operations Manager that will be acceptable to implement outside of the process. Verbal or written approval must be obtained. Requests approved outside of the normal process will require the requestor to notify the Operations Supervisor, Help Desk Manager, or the Help Desk Supervisor. This notification should not occur via email or voice mail. The appropriate change documents must follow any change that is granted an exception within one business day of the change being completed. Documentation should be placed in the "Change Bin."

- C. Scheduled preventative maintenance does not need to follow this process. Scheduled preventative maintenance performed by Tech Support is defined in a separate document.
- D. System tuning does not need to follow this process. The Help Desk will be notified when system tuning is done.

Requirements

- A. All changes must be accompanied by a list of components that are changing, along with the description of the change.
- B. All changes must provide a list of affected applications/hardware that interface with the changed component.
- C. Patches and vendor-related changes require a summary of what is changing and how it impacts our environment.
- D. Detailed implementation plan requires an estimated time frame by task (including backout requirements).
- E. Detailed validation procedures require estimated time frames (executed after production moves to ensure changes were implemented correctly).
- F. Changes introducing new files or equipment require documentation on the backup procedures and disaster recovery requirements.

Change Requirements for Vendors

- A. Changes applied to a vendor-supported system will follow the change process as defined.
- B. All changes to a vendor supported production system must be coordinated with the established I.S. contact for that vendor.
- C. The I.S. contact will ensure that the documents have been submitted to the "Change Bin" and that the timelines for the change are communicated to the vendor.
- D. The I.S. contact is responsible for ensuring that the customer or customer representative is involved in planning, testing, and implementation, and ensures that the vendor does not make or implement changes without going through the Change Control Process.
- E. Fund I.S. personnel will provide the necessary password to the vendor for dial-in purposes. Fund I.S. personnel will modify the password upon completion of the vendor's work. The I.S. contact responsible for the change will ensure any passwords are modified.
- F. The I.S. contact will coordinate the vendor's efforts to ensure the appropriate party is onsite at headquarters during vendor activity.

FYI:**Production System**

- Monday - Friday: 7:00 A.M. - 7:00 P.M.
- Saturday: On Request
- Sunday: On Request

Maintenance Timeframe

- Available for IS maintenance activities daily between 7:00 P.M. and 7:00 A.M.
- Available for IS maintenance activities on weekends between 7:00 P.M. Friday and 7:00 A.M. Monday.

Note: Maintenance activities that require hours outside of the specified window will be granted on a special request basis by the Production Services Sr. Manager.

ADRS:**Production System**

- Monday - Friday: 8:00 A.M. - 11:30 P.M.
- Saturday: On Request
- Sunday: On Request

Maintenance Timeframe

- Available for IS maintenance activities daily between 11:30 P.M. and 7:00 A.M.
- Available for IS maintenance activities on weekends between 11:30 P.M. Friday and 7:00 A.M. Monday.

Note: Maintenance activities that require hours outside of the specified window will be granted on a special request basis by the Production Services Sr. Manager.

**Client Server
Applications:****Environment Available**

- Monday - Friday: 7:00 A.M. - 7:00 P.M.
- Saturday - 7:00 A.M. - 7:00 P.M.
- Sunday - 7:00 A.M. - 7:00 P.M.

Important: Due to system maintenance activities, there are times this environment will not be available on Sundays. When this is the case, advanced notice will be sent to all users to make them aware of the affected timeframes.

Maintenance Timeframes:

Available for IS maintenance activities daily (including weekends) between 7:00 P.M. and 6:00 A.M.

Note: Maintenance activities that require hours outside of the specified window will be granted on a special request basis by the Production Services Sr. Manager.

Scheduling Operations Coverage

To schedule Operations coverage for special support during off hours, the Computer Operations Supervisor or Resource Administrator will need to be notified no later than Wednesday, close of business. Requests made after that time will be subject to approval from the Computer Operations Supervisor.



Attorneys' Title Insurance Fund, Inc.
POLICIES/PROCEDURES

Subject: On-Call Compensation	Effective Date: 11/1/98
--------------------------------------	--------------------------------

Authorized by: J.H. Clark

Title: SVP, Information Services

Revised: 11/1998

Purpose: The purpose of being on call is to provide adequate backup in all support areas for critical production systems/applications. The objective is to set forth guidelines for compensation and expectations for employees involved in the on-call rotation. The On-Call Compensation Policy will ensure that employees are compensated for providing on-call support, 24 hours per day, seven days per week, Monday through Sunday (not to exceed two consecutive weeks under routine circumstances; exceptions may occur). This does not pertain to project or special task activity that requires off-hours involvement. These on-call rotations are planned and scheduled in advance.

Policy: Compensation

Information Services employees who are required to carry a pager for after hours or weekend support of critical production applications will be compensated \$50.00 per week for hourly and \$75.00 per week for salaried employees. In the event that hourly employees are called in, they will be paid for a minimum of four hours. The pay for being on call will be included in the employee's regular pay cycle.

Expectations

Employees on call are required to remain sober and in a ready state of mind to report to work. Employees on call must remain within the metropolitan area of their primary on-call site. Employees who live outside the metropolitan area must remain reachable by pager and within a distance that does not exceed their normal commute to work.

Requirements

- Information Services management must identify systems/applications requiring after hours support.
- Information Services management must examine each unit's support responsibilities.
- Each unit manager must identify individuals who can provide support.
- Each unit manager must have on-call rotation schedules and lists for Operations.
- Each unit manager must develop cross-training plans to remedy areas of support that are dependent on one individual.



Attorneys' Title Insurance Fund, Inc.
POLICIES/PROCEDURES

Subject: Production Problem Management Process	Effective Date: 04/22/02
------------------------------------------------	--------------------------

Authorized by: J. Calabrese Title: SVP, Information Services New/Revised:

Purpose: The objective of the Problem Management Process is to ensure that all problems are identified, documented, and assigned the appropriate priority (severity level) based on impact to the business or our customers, and resolved in a timeframe that supports our commitment to customer service.

Policy: It is a policy of The Fund that all problems in the Production environments are required to go through the Problem Management Process. This process is performed by identifying and assigning all problems at the daily Problem Management Meeting.

Severity Codes (Critical / High / Medium/ Low)

Critical – A complete failure of an application/hardware/software/network component. No work-around is available; the problem presents the risk of returning inaccurate results, and may increase chances of claims, or prohibit a user or department from accomplishing crucial tasks that jeopardize The Fund's Quality & Services Guarantee Policy. Immediate notifications are made to the key contacts of the failing components. Information Services is committed to finding the quickest possible resolution, and problems are reviewed each morning in the Problem Management meeting until they are resolved. If a critical problem is not resolved within one hour, it will be escalated to the appropriate I.S. and customer management to ensure that the focus remains on resolving the issue.

High – A failure of an application/hardware/software/network component that impacts user productivity and delivery of products or completion of crucial tasks in a timely manner. These problems have no threat to the Quality Services Guarantee, but can potentially impact the users' abilities to meet their Service Goals. These problems will be discussed each morning in the Problem Management Meeting and will remain in focus until resolved or downgraded. If a high problem is not resolved within two hours, it will be escalated to the appropriate IS and customer management to ensure the focus remains on resolving the issue.

Medium – An application/hardware/software/network component failure that needs attention but has a work-around in place or is not impacting the user from completing or delivering crucial tasks. The issues will be resolved as resources are available by the assigned group.

Low – A general failure that needs to be brought to attention but is not impacting the business in any way and may be worked as resources are available.

Procedures: ***Initial Call*** – The person taking the initial call must ensure that the impact to the customer is understood and that the customer is aware of the assigned severity. If the customer is not in agreement with the assigned severity, they should elevate their concern to their manager or IS manager.

New Problem – All problems are to be documented online with the appropriate severity level and introduced at the Daily Problem Meeting via Report. The person opening the problem must give a description of the problem, the customer being impacted, and an explanation of the impact to the customer. All new problems are subject to questions attempting to further clarify the problem description, to ensure correct severity level and for proper assignment for quickest resolution.

Tracking/Monitoring – All problems that are assigned a critical or high severity level will be discussed in the morning meeting. Department managers and/or designees are responsible for daily updates to all critical and high problems in the reporting system and must be able to discuss them in the morning meetings. Medium and low problems are also documented and worked as resources are available.

Closing Problems – All problem tickets that have been corrected are to be updated with the cause, resolution, name of the individual who resolved the problem, department the individual reports to, date of resolution, and details of the actions taken. The individual who resolved the problem should then assign the IR for closure within Applix. Production Operations (The Help Desk) will verify the information for accuracy, completeness, and validity. The Help Desk will then follow up with the user/customer to ensure that the problem was resolved to their satisfaction. Information should be available for communicating to the customer, including what caused the problem, whether the fix was permanent or temporary, and what was done to resolve the problem, as well as any user documentation requirements as part of the fix.

Meetings: Daily Problem Meeting – (Monday – Friday, 09:30 AM – 10:00 AM)

A daily meeting is conducted to review new problems and update the status of critical and high problems. This approach is intended to ensure that the management or designees attend the meetings, remain focused on obtaining a resolution to critical and high problems, are able to state the progress and status of open problems, and ensure that the appropriate severity is assigned to new problems. All problems discussed in this meeting are subject to questions attempting to make certain that the suitable resources and priority have been assigned.

It is important that our objective is to ensure that problems are resolved. We will also review any request to upgrade or downgrade problems based on user impact, length of time the problem has been opened, and occurrence count. All requests will be considered, and if approved for upgrade, it becomes the unit manager's responsibility to ensure that the problem is given the appropriate resources to resolve. Problems cannot be downgraded without prior notification and acceptance by the user/customer. This is a mandatory meeting and must have a representative from each group daily.

Weekly Production Operations Problem Meeting – (Friday)

The Production Operations Manager will meet with the Support Services Manager, Help Desk Manager, and Computer Operations Supervisors to go over the weekly problems and decide on courses of action for open or chronic issues.



Attorneys' Title Insurance Fund, Inc.
POLICIES/PROCEDURES

Subject: Production Problem Analysis Report Process	Effective Date: 11/2/98
------------------------------------------------------------	--------------------------------

Authorized by: J. H. Clark Title: SVP, Information Services New/Revised: New

POLICY: It is the policy of The Fund that a Production Problem Analysis Report (PPAR) be created and presented to I.S. Management upon the resolution of a production problem. The area manager assigned to the problem is responsible for ensuring that this is accomplished within the guidelines of this policy.

Problems that are documented as not having an acceptable resolution or pending vendor upgrade, and have been approved/accepted by the Problem Management Process, are excluded from the Problem Analysis Process.

GUIDELINES

- Problems that result in an impact or outage to the customer in excess of one hour will require a PPAR.
- The PPAR will be segregated into sections describing what happened, why it happened, and how to prevent reoccurrences in the future. The business area impact will be completed by the Help Desk and attached with the PPAR prior to management's review. See the attached examples for formatting and content.
- The PPAR will be used for Production systems only. Systems that are used for testing or development are specifically excluded from the scope of this policy.
- The submission of the PPAR is required within 3 working days of the resumption of service.
- The PPAR will be addressed to the Production Operations Manager and the responsible Area Manager.
- Production Operations will review the document to ensure it meets the requirements. If necessary, time will be scheduled with the Director of Information Services to review the results, including time frames on any action items assigned for follow-up.
- The Area Manager assigned a specific task as a result of the analysis process is accountable for follow-through and status updates on the progress of the task through implementation.

PROCEDURE: A PPAR will be written if a production problem causes a service outage of one hour or more, or if requested by the Production Operations Manager or Director of Information Services. The PPAR, including the Impact to the Business Assessment, will be submitted to the Production Operations Manager with a copy to the Area Manager via Email within three working days of the resumption of service. A face-to-face meeting may be required at the discretion of the Production Operations Manager or Director of Information Services. Once the Director of Information Services accepts the PPAR, the PPAR will be posted to a public Email folder.

EXCEPTIONS: Exceptions to this policy may occur based on a specific instance or customer impact. However, exceptions will be requested directly by the Production Operations Manager or the Director of Information Services.

PRODUCTION PROBLEM ANALYSIS REPORT

1.0 The Problem

This section should annotate the details of the production outage. The explanation should include the date/time of the beginning of the outage, the date/time of the resumption of service, and the affected systems/services.

2.0 The Cause

This section should annotate the cause of the service outage.

3.0 The Future

This section should annotate any actions that can be taken to prevent such an occurrence in the future.

Submitted by: _____

Date: _____

BUSINESS UNIT IMPACT REPORT

1. Impact to the Business Unit

This area describes the impact to the customer's service goals and/or other established agreements. If the outage resulted in refunds or waived charges, the total dollar impact should be shown in this area.

Submitted by: _____

Date: _____



Attorneys' Title Insurance Fund, Inc.
POLICIES/PROCEDURES

Subject: Computer Hardware and Software Standards Effective Date: 05/03/05

Authorized by: J. Calabrese Title: SVP, Information Services New/Revised: New

Purpose: The purpose of this policy is to implement a standard for computer hardware and software used throughout The Fund. This will reduce the total cost of ownership and increase overall reliability (*total cost of ownership includes support, maintenance, supplies and the initial cost of the product*).

Policy: Based on the business needs, The Fund will provide Personal Computers (PC's) and Peripherals (*i.e. network printers, direct connect printers and other PC accessories*). In order to provide a secure environment and consistent, reliable support for this equipment it is the Policy of The Fund that this equipment will adhere to technology standards as approved by the Technology Oversight Group (TOG). The purchase and use of computer hardware and software used within The Fund will comply with these standards (*documentation is located under the "J:\Shared\Technology Oversight Group" directory*). It is the Policy of The Fund that all PCs will be deployed with the standard desktop configuration as defined in the Desktop Standards Configuration Document (documentation is located at <http://intranet.thefund.com/desktop/docs/index.htm>).

Procedure:

1. A STARS Request (S/R) will be generated to request computer hardware and/or software.
2. The completed STARS request will be sent to the user's manager for approval and will be routed to Support Services for processing.
3. Support Services will identify the standards in place for computer hardware and/or software requests and generate an order to purchase from the approved vendor.
 - a. Any STARS request requesting computer hardware and/or software that has not yet been approved for use must be routed to Technical Services to be tested for compatibility and forwarded to TOG for approval.
4. Support Services will accept delivery for the order.

5. Support Services will notify user and coordinate the install/set-up of the computer hardware and/or software.
 - a. All new software will be routed to Technical Services to set-up the remote installation of the software. Support Services will install all software through the remote software installer tool.
6. Support Services will close the STARS request after the computer hardware and/or software has been installed successfully.



Attorneys' Title Insurance Fund, Inc.
POLICIES/PROCEDURES

Subject: Software Inventory Policy

Effective Date: 08/03/03

Authorized by: J. Calabrese

Title: SIP, Information Services

New/Revised: New

Purpose: The purpose of this policy is to implement a standard for all workstations and servers running on the following listed software programs or using client access licenses for these programs.

Policy: To ensure licensing compliance with Microsoft's Enterprise Agreement including the following products:

- Windows Workstation (3.1, 3.11, '95, '98, ME, NT3.51, NT 4.0, 2000, XP)
- Windows Server NT, 2000, 2003
- Windows Advanced Server NT, 2000, 2003
- MS Office (including any of the following: Word, Excel, PowerPoint, Access, Outlook)
- MSDN Universal Win32 SA
- Project Pro
- Project CAL
- Project Server
- Visio Pro
- Visio Standard
- Exchange Server Enterprise
- SQL Sever Standard Edition
- SQL Sever Standard Edition Processor License
- System Management Server Enterprise Edition
- Windows Terminal Server Client Access License's.

Procedure:**Physical Inventories**

Every March and September, Support Services will perform an inventory of PC's and Servers at The Fund. This inventory is to be completed and submitted no later than on the last working day of the month in which it was started. The September inventory will consist of walking to each PC and collecting the PC's asset tag number and End Users name on an ATIF inventory sheet (see appendix A) or keying the number and name into a database. The March inventory will also include a physical audit of the above listed software on each PC. In the case of servers, the name of the server will be captured indicating its physical location. The inventories of servers and PC's will be completed at the same time but are to be compiled separately. The end product of the inventory will consist of two spreadsheets. One will total the number of PC's indicating which of the above listed Microsoft software is running on them (for the March inventory only) and one totaling the number of file servers and their locations. Servers with a VM designation (this will be clearly marked on the front of the server) have more than one host running on them. As such they are a special case and support services will work with technical services to determine the total number of virtual servers running on each of these for an accurate license count.

If these inventories are unable to be completed in the designated time, then a written explanation must be supplied to the Support Services Manager. The Support Services Manager is then to report this reason to the Technical Support Manager.

Asset numbers are to be collected and grouped by location. For example, a collector would start in a branch or if at headquarters policy operations as an example, and collect all the data in that location and move to the next location.

If any branch or data center is not in a technical services hardware/software inventory database, then the physically collected inventory data keyed into the spreadsheet will be considered the final and true inventory for that location.

ATIF Inventory sheets (or the format of the inventory collection sheets if a laptop or barcode scanner is used) are to be used in the collection of this data. A sample of these sheets is provided at the end of this document. (See Appendix A)

The data, once collected, is to be keyed into a spreadsheet by support services.

For the March inventory, Support Services will annotate the spreadsheet indicating which of the PC's use Microsoft software components (Word, Excel, PowerPoint, Access Visio or Project) and which are devoid of these components. If any PC has any one of these components then that PC will be said to be an "office automation" PC and so annotated on the spreadsheet. The PC's that have no MS Office components on them or Project or Visio will be so annotated on the spreadsheet as "Line of Business". Please see the sample spreadsheet in Appendix A.

When the spreadsheets have been completed, technical services will be notified via e-mail and the asset numbers reconciled to the technical services hardware/software inventory database.

When the data collection and update of spreadsheets is complete and has been reconciled to the technical services database, the final numbers will be e-mailed to the Branch and/or Data Center Managers, Distributed Systems Supervisor and the Support Services Supervisor.

These numbers will be used as a count to compare what is currently owned in Microsoft products vs. the number of Microsoft product licenses owned. These numbers will be used to "True-Up" the Microsoft enterprise agreement that is currently in place.

Reconciliation of Data

Data is to be reconciled by technical services against the technical services hardware/software inventory database.

The assigned technical services administrator will run software inventory reports displaying what software is running on each PC.

The assigned technical services administrator is to rely on the compiled physical inventories and the data available from the databases to come to consensus on the number of PC's and servers at The Fund and the type of software being run on these machines.

This compiled data is to be delivered in the form of:

- Number of PC's
- Number of PC's running Visio
- Number of PC's running Visio Pro
- Number of PC's running Project
- Number of PC's running Project Pro
- Number of PC's running Microsoft Office
- Total Number of Office Automation PC's
- Number of PC's not running Office, Project or Visio.
- Total Number of Line of Business PC's
- Total Number of Servers and the OS version of software running on each server

The Distributed Systems Supervisor will use this as the "official count."

The Distributed Systems Supervisor will supply the current-licenses-owned count and the current-license-in-use count to the Technical Services Manager. The Distributed Systems Supervisor will also supply the counts to the Support Services Supervisor who will insure we are in compliance with our Microsoft licensing agreement.

All effort will be made to eliminate old PC's through retirement and attrition. The focus of this effort will be to keep our total EA license count as low as possible. This will help eliminate the need to purchase additional EA licenses in the future.

Appendix A

ATIF PC Inventory Sheet								
Office:	Broward							
Department:								
Floor:								
PC Asset Tag	User	Office	Project	Project Pro	Visio	Visio Pro	Office Automation	Line of Business
L0004186	John Doe	Y					Y	N
L0004189	Jane Doe	Y	Y			Y	Y	N
L0004250	Jim Smith						N	Y

ATIF Server Inventory Sheet	
Server Name	Location
ORLFS1	HQ
DADFS1	Dade
DADPS1	Dade



Attorneys' Title Insurance Fund, Inc.
POLICIES/PROCEDURES

Subject: Standardized Desktop Policy

Effective Date: 01/20/03

Authorized by: J. Calabrese

Title: SVP, Information Services **New/Revised:** New

Purpose: The purpose of this policy is to establish a standard user PC to reduce the total cost of ownership and increase their overall reliability. The Fund will respect all computer software copyrights and adhere to the terms of all software licenses for approved software being used within The Fund.

Policy: It is the policy of The Fund to provide Personal Computers (PC's) as needed within the Company and to provide consistent and reliable support for these computers. In an effort to support these computers, a Standard Desktop has been configured for all employees. The Standard Desktop includes the hardware configuration of the PC, a standard operating system and approved applications that are deployed to all employees. The Fund's PCs are deployed with a pre-defined security setting approved by I/S and Fund Management. Only approved software will be installed on a user's PC. All approved software will be deployed via a remote install process, if possible. This remote install process will ensure the correct version of software is being deployed to all users.

In defining the Standard Desktop within The Fund, the reliability of the PC's will increase and the production losses and costs to maintain each PC will decrease.

The scope of this policy includes all PCs and users within The Fund (with the exception of those identified within this document) and all Software and Hardware that is owned and being used for Company purposes.

General

- Standard Desktop and Laptop Hardware is approved by the Standard Architecture Review Committee (SARC). The SARC Documentation is located at: J:\Shared\SARC\Presentation\2002 (The 2002 directory reflects the year the SARC presentation was created and approved.)
- The 'Core Load' for all PC's consists of the Windows 2000, Windows XP and future Microsoft Operating Systems, McAfee VirusScan, McAfee ePolicy Orchestrator (ePO), SMS, and Adobe Acrobat Reader with search capabilities. The Core Load is defined within the Standard Operating Environment [SOE] Document. The Core Load is available through RIS (Remote Install Service) and is installed by the Field Engineers.
- The Core Load installed on all PC's cannot be changed. Requests for updates to the Core Load will be processed through a STARS request. The Core Load will be installed on every PC.
- Software installed as part of the Core Load will not be deleted from any PC.

- There will be scheduled periodic updates to the Core Load and these updates will be tested by the Test Team before being available for deployment.
- All internally developed software must be tested by the Test Team and approved by the SARC Committee prior to being deployed to a user.
- All off-the-shelf software will be approved by the SARC Committee prior to being deployed to a user and will be available for remote deployment via a Vendor Supplied MSI package. (Not all off-the-shelf software comes with the ability to remotely install. Evaluation of off-the-shelf software must consider the ability to remotely install the software.)
- All internally developed and off-the-shelf software packages that are deployed to any user will be placed in the Software Installer Tool. Field Engineering is solely responsible for installing all software. This includes, but is not limited to, software delivered by CD, diskette, internal networks and the internet. (This does not apply to those users listed as Standard Desktop Exceptions. See section 1.4.2.2.)
- All Desktop PC's must be left on overnight. Users are required to log-off the PC, and will leave the PC on. (Laptop PC's are not required to be left on overnight, however, the Laptop will not receive automatic updates until the Laptop is turned on and connected to our network)
- Users are not authorized to install software. (This does not apply to those users listed as Standard Desktop Exceptions. See section 1.4.2.2.)
- Software must be purchased by the use of a properly completed STARS request.
- Licensing compliance will be verified prior to fulfilling any request for software installation. This includes set up of a new PC, new software ordered, moving software from one PC to another, and IRs that involve software installation.
- All software installed on any PC will comply with the computer software copyrights and licensing requirements.
 - Validation of licensing is required for all user software. The Fund has software covered by a site license, enterprise agreement, or purchased in block quantities and is not subject to proof of ownership. See Attachment A for list of software that is included.

Guidelines: Approved Software

- Approved Software is reflected on the BRICKS and/or the Application Data Collection list (J:Shared/BRICKS/ATIF BRICKS and J:Shared/BRICKS/Approved SW List).
- To request new software not already available, a STARS request will be created and approved by Management. Once the request is reviewed and approved by the SARC Committee, the new software can be tested and packaged for remote deployment.

Standard Desktop Exceptions

- Exceptions are defined in the Standard Operating Environment (SOE) Document.
- Additional exceptions will be reviewed and considered. Any requests for additional exceptions will be forwarded through a STARS request to Tech Support. Final approval of all exceptions will be made by the Technical Support Manager.
 - If there is a critical need for an additional exception, a temporary exception can be granted pending final approval. The Temporary exception will be revoked within one week.

Standard Desktop Security

- The Standard Operating Environment (SOE) Document is located in the J:\Shared\StandardsCommittee\Final_Standards folder. This document defines specific PC configurations for our standard user.

Enforcement: Any employee found to have violated this Standardized Desktop policy may be subject to disciplinary action, up to and including termination of employment.

Definitions:

PC	Personal Computer – A desktop or laptop computer that is owned by The Fund and in use by an employee within The Fund for business purposes only.
SARC	Strategic Architecture Review Committee – This Committee reviews and approves new Software for use within The Fund.
SOE	Standard Operating Environment – The Standard Operating Environment Document describes Standards that were defined for all PCs in use by The Fund.
RIS	Remote Install Service – The process and service being used to install Operating Systems and core applications to PCs in use by The Fund.
BRICKS	A document that defines the Architecture being used within The Fund.
Applications Data Collection List	A list of all Approved Applications in use within The Fund.
Computer Acceptable Use Policy	A Policy written defining acceptable use of Company-Owned Computers.
Core Lead	A pre-tested configuration that includes an operating system and selected applications approved for installation on all Fund PCs.
Software Installer Tool	A Tool that was created, tested, and approved to deploy applications to all users at The Fund.
Field Engineers	The individuals that setup, install, and deploy PCs to users at The Fund.
Standard Operating Environment Document	An approved document that describes Standards that are used for all PCs in use by The Fund.

STARS	An application that is used to request hardware and/or software.
EPO	McAfee ePolicy Orchestrator is an Antivirus application for Windows 2000 and Windows XP PCs.
SMS	Software Management Service
I/S	Information Services Department
I/Rs	Incident Report

Revision History:

Date	Version	Description	Author
9/8/02	Draft - 1.0 – 1.4	Document Drafts –routed for review	Bonnie Jean
9/8/02	Draft - 1.4	Final Draft submitted for Sponsor Approval	Bonnie Jean
12/2/02	Draft - 1.5	Incorporate Sponsor Changes	Bonnie Jean
1/7/03	Draft - 1.6	Incorporate additional Sponsor Changes	Bonnie Jean
1/20/03	1.0	Incorporate template header on cover page of document. Add approval for all exceptions by Tech. Support Manager in section 1.4.2.2	Bonnie Jean
4/5/04	1.1	Added PDA Addendum to this document	Bonnie Jean

Subject: Addendum – Standardized Desktop Policy – Personal Digital Assistant
Effective Date: 03/29/04

Authorized by: J. Calabrese Title: SVP, Information Services New/Revised: 04/05/04

Purpose: The purpose of this policy is to establish guidelines for PDA use within The Fund. These guidelines will reduce risks associated with PDA virus attacks and will reduce the total cost of support.

Policy: General

- PDA hardware and software will comply to the Standards defined herein.
 - The Criteria defined for PDA devices purchased and supported by The Fund must be met.
-

Guidelines:

Business Criteria for use of PDA devices

- The employee travels a significant amount (40-50%) of the time or an average of 2-3 days per week.
- The employee's position requires that they work remotely (e.g., Sales Rep).
- The employee is required to support critical applications or systems after normal business hours.
- The Senior Vice President of Information Services must approve the purchase of all Fund-Owned Devices

Fund-owned and Supported Devices

- Fund-Owned Devices will ONLY be MS Pocket, PC-based Devices manufactured by DELL, Compaq, or Toshiba.
- ActiveSync software by Microsoft v 3.5 or greater.
- The most current Fund-approved version of PDA anti-virus software must be installed on the user's PC.

Personally-Owned Devices

- An employee can connect their personal PDA to a Fund PC only if they purchase and schedule the installation of the most current Fund-approved version of PDA anti-virus software on their PC.
- The Fund will not support the PDA; however, Support Services will provide limited support on The Fund PC, for the installation of PDA and anti-virus software.

Attachment A**Software exempt from proof of ownership:**

- Adobe Acrobat Reader
- Applix
- DoubleTime
- FIT
- FYI
- ILV
- Internet Explorer
- Karma
- Lawson
- LED
- McAfee
- Microsoft Office (does not include Project)
- Operating Systems
- Oracle
- PROS
- Reflection
- SDE
- SMS
- STARS
- TIPS



Attorneys' Title Insurance Fund, Inc.
POLICIES/PROCEDURES

Subject: Reproduction of PC Software

Effective Date: 10/01/89

Authorized by: Joseph Kolman Title: SVP, Information Services New/Revised: New

Purpose: There have been questions about whether or not it is permissible to copy software from one PC for use on another. This is not only illegal, but could cost The Fund a great deal of trouble and money. According to the U.S. Copyright Law, illegal reproduction of Software is a Federal offense. Civil damages for unauthorized software copying can be as much as \$50,000 or more, and criminal penalties include fines and imprisonment.

The Fund licenses the use of its computer software from a variety of outside companies. The Fund does not own this software or its related documentation, and unless authorized by the software developer, does not have the right to reproduce it.

The Fund has therefore instituted a policy that prohibits the illegal duplication of computer software. If a software package is used on a regular basis, then a licensed copy of the software must be purchased.

If there are any questions as to what software may or may not be copied, please contact the PC Support department.

Policy: It is the policy of The Fund that all PC software programs that are used on a regular basis shall be authorized licensed copies rather than reproductions of the original program.



Attorneys' Title Insurance Fund, Inc.
POLICIES/PROCEDURES

Subject: Computer Acceptable Use Policy – Rev 2.0

Authorized by: Jeannie Calabrese Title: SVP, Information Services Revised: 12/09/05

Purpose: The purpose of this policy is to outline the acceptable use of computer equipment at Attorneys' Title Insurance Fund, Inc. These rules are in place to protect the employee and The Fund. Inappropriate use exposes The Fund to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope: This policy applies to employees, contractors, consultants, temporaries, and other workers at The Fund, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by The Fund.

Policy: General Use and Ownership

- It is the policy of Attorneys' Title Insurance Fund, Inc. that ALL Internet communications, emails and web/ftp/messaging/streaming, will be monitored and logged at all times. There is no right to privacy on any Fund computer system or system operating on Fund property.
- Users should be aware that the data they create on the corporate systems remains the property of The Fund. Furthermore, that these systems are intended for business use.
- Management reserves the right to prohibit employee access to the Internet at any time.
- All levels of management share responsibility for ensuring the Internet users with their organizations abide by these policies.
- For security and network maintenance purposes, authorized individuals within The Fund may monitor equipment, systems and network traffic at any time, in accordance with The Fund's Audit Policy.
- The Fund reserves the right to audit networks, systems and PCs on a periodic basis to ensure compliance with this policy.
- In order to provide better support to our users, ALL PCs will be left on at all times. The user should log out at night, however, do not shutdown your PC.

- Blogging during company time should be regarded as web use during company time and is covered under acceptable use. It should be further understood that when blogging using your Fund account, you are a representative of the company whether you intend to be or not. Entries into blogs during company time should be related to company business and in no way discredit The Fund or our customers.

Security and Proprietary Information

- Password use and creation must be in accordance with The Fund's Employee Network Computer Password Policy.
- It is highly recommended that all PCs, laptops and workstations be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (Windows Button – L for XP) when the desktop will be unattended.
- Because information contained on portable computers is especially vulnerable, special care should be exercised with the physical security of the laptop. Always be aware of your surroundings when carrying a laptop to prevent theft.
- Postings by employees from The Fund email address to newsgroups will only be done when it is in the course of business duties.
- All systems (desktop/laptop and server) used by the employee that are connected to The Fund Internet/Intranet/Extranet, whether owned by the employee or The Fund, shall be continually executing approved virus-scanning software with a current virus database.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

- Under no circumstances is an employee of The Fund authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing The Fund-owned resources.
- The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by The Fund.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which The Fund or the end user does not have an active license is strictly prohibited.
- Illegal exporting of software, technical information, encryption software or technology, in violation of international or regional export control laws. Appropriate management must be consulted prior to export of any material that is in question.
- Intentional introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Password use must be in accordance with The Fund's Employee Network Computer Password Policy.
- Using a Fund computing asset (PC or server) to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any Fund account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless this activity is a part of the employee's normal job/duty.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.

- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Installing any software not approved by The Fund and installed in a manner prescribed by Technical Services on any server or workstation.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, Fund employees to parties outside The Fund.
- Disabling any portion of the core desktop environment:
 - Antivirus
 - Desktop management systems – McAfee EPO
 -

Revision History

Date of Rev	Update Made	Made By
12/9/05	Added verbiage concerning blogging	Nick Patellis
12/9/05	Rev 2.0 into new format	Nick Patellis



Attorneys' Title Insurance Fund, Inc.
POLICIES/PROCEDURES

Subject: PC Inventory	Effective Date: 6/00
------------------------------	-----------------------------

Authorized by: J. Calabrese **Title:** VP, Information Services **New/Revised:** New

POLICY: It is the policy of The Fund to perform six-month PC Hardware inventories to insure compliance with Microsoft's Enterprise Agreement.

PURPOSE: To ensure licensing compliance with Microsoft's Enterprise Agreement including the following products:

- Microsoft Office Professional (MS Word, PowerPoint, Excel & Access)
- Windows (3.1, '95, '98, NT3.51, NT 4.0 & Windows 2000 Professional)

PROCEDURE: The following are guidelines and/or procedures that must be adhered to in support of the policy statement and objective.

Physical Inventories

Every March and September, Support Services will perform a physical inventory of PC's at The Fund. This inventory is to be completed and submitted no later than on the last working day of the month in which it was started. This inventory will consist of walking to each PC and writing the PC's asset tag number and End Users name down on an ATIF inventory sheet or keying the number and name into a database.

If this inventory is unable to be completed in the designated time, then a written explanation must be supplied to the Support Services Manager. The Support Services Manager is then to report this reason to the Technical Support Manager.

Asset numbers are to be collected and grouped by location. For example, a collector would start in a branch, or if at headquarters policy operations as an example, and collect all the asset tags in that location and move to the next location.

Please see the Spreadsheet located at:
"J:\Shared\Projects\SysMgmt\PC Inventory\PC Inventory.xls"
for exact groupings.

If any branch or data center is not in the SMS database, then the collected inventory data keyed into the spreadsheet will be considered the final representation of the true physical inventory.

ATIF Inventory sheets (or the format of the inventory collection sheets if a laptop or barcode scanner is used) are to be used in the collection of this data. A sample of this sheet is provided at the end of this document. See Attachment #1

The data, once collected, is to be keyed into a spreadsheet by support services. Care should be taken to insure the data is input under the correct tab (HQ, Dade, Duval, etc) The spreadsheet is located at:

"J:\Shared\Projects\SysMgmt\PC Inventory\PC Inventory.xls".

Support Services will annotate the spreadsheet indicating which of the PC's uses Microsoft Office components (Word, Excel, PowerPoint or Access) and which are devoid of MS Office components. If any PC has any one of these components then that PC will be said to be an "office automation" PC. The PC's that have no MS Office components on them will be so annotated on the spreadsheet as "Line of Business". The PC's with office components do not need to be annotated. Please see the sample spreadsheet at the end of this document.

When the spreadsheet has been completed, the Technical Support SMS Administrator will be notified via e-mail and the asset numbers reconciled to the SMS database.

When the data collection and update of spreadsheets is complete and has been reconciled to the SMS database, the final numbers will be e-mailed to the Branch and/or Data Center Manager, Distributed Systems Supervisor and the Support Services Supervisor.

These numbers will be used as a count to compare what is currently owned in Microsoft products vs. the number of Microsoft product licenses owned. These numbers will also be used to "True-Up" any Microsoft software licensing contract that is currently in place.

Reconciliation of Data

Data is to be reconciled by a Technical Support SMS Administrator.

The SMS Administrator will run software inventory reports from SMS displaying what software is running on each PC.

The SMS Administrator is to rely on the compiled physical inventories and the data available from the SMS database to come to consensus on the number of PC's at The Fund and the type of software being run on these machines.

This compiled data is to be delivered to the Distributed Systems Supervisor in the form of:

- Number of PC's
- Number of PC's running Microsoft Office Applications
- Number of PC's running line of Business applications (main frame access, imaging PC's etc.)

The Distributed Systems Supervisor will use this as the “official count” to insure we are in compliance with our Microsoft licensing agreement.

The Distributed Systems Supervisor will supply the current-licenses-owned count and the current-license-in-use count to the Technical Support Manager.

All effort will be made to eliminate old PC's through retirement and attrition. The focus of this effort will be to keep our total EA license count below the 1000 level. This will eliminate the need to purchase additional EA licenses.

SAMPLE ATIF Inventory Sheet

Located at: J:\Shared\Projects\SysMgmt\PC Inventory\PC Inventory.xls

ATIF Inventory				
Office:	DADE			
Department:				
Floor:				
PC Asset Tag	User	Line of Business Y/N		
L0004186	John Doe	Y		



Attorneys' Title Insurance Fund, Inc.
POLICIES/PROCEDURES

Subject: Remote Access Policy	Effective Date: 07/12/05
-------------------------------	--------------------------

Authorized by: Jeannie Calabrese Title: SVP, Information Services Revised: 6/27/05

Purpose: The purpose of this policy is to provide The Fund's policy on connecting Fund-owned computers to remote non-Fund owned systems via dialup/modem, and connecting remote systems (Fund owned or not) to our systems.

Policy: This policy covers all computers owned or operated by The Fund. All modems used on any Fund PC must be configured for dial out only.

The following groups are authorized to have dial-out capability:

- Test team
- Help desk
- Branches requiring dial-out to support Fund business
- Technical Services

Users requesting this type of service must submit a STARS request.

Procedure: **Remote Fund Laptops Connecting to Fund Systems**

- Fund laptops can utilize Remote Access Services (RAS) if required or utilize Virtual Private Network (VPN) to connect to The Fund's terminal server system.
- All traffic will be monitored for compliance with The Fund's Acceptable Use Policy.

Users requesting this type of service must submit a STARS request.

Remote Non-Fund Owned PCs Connecting to Fund Systems

- VPN access will be provided to Fund employees and contractors as requested by their managers.
- Connectivity will be to terminal services only.

Users requesting this type of service must submit a STARS request

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Date of Revision	Update Made	Made By
June 27th, 2005	Initial document	Nick Patellis



Attorneys' Title Insurance Fund, Inc.
POLICIES/PROCEDURES

Subject: Employee Network Computer Password Policy	Effective Date: 08/02/04
----------------------------------------------------	--------------------------

Authorized by: J. Calabrese Title: VP, Information Services New/Revised: New

PURPOSE: Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of The Fund's entire corporate network. As such, all Fund employees (including contractors and vendors with access to Fund systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

POLICY: The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any network system that resides at any Fund facility, has access to the Fund's network, or stores any non-public Fund information.

General Guidelines

Password requirements for LAN (Network, NT, Windows XP, etc.) at Attorneys' Title Insurance Fund, Inc. are as follows:

- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed every four months (120 days).
- **The user will be prompted by the system to change passwords.**
- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed every three months (90 days).
- All production system-level passwords will be kept in the Operations safe.
- Passwords must be at least eight (8) characters long.

- Passwords must contain characters from at least three (3) of the following four (4) classes:
 - English upper case letters, A,B,C...etc
 - English lower case letters, a,b,c,...etc
 - Numbers, 1,2,3,...etc
 - Special characters, !@#\$%^&*()_+|~-=\`{}[]:"';'<>?,./)

Example:

5spaceCadet – acceptable password as it contains upper case, lower case and a number.

M!ckeymouse – acceptable password as it contains upper case, lower case, and a special character (exclamation point).

spaceCadet – unacceptable password

- Passwords may not contain your user name or any part of your full name.
- Password reuse is not allowed for a period of six password changes.
- Passwords cannot be changed within seven (7) days of previous change.
- Users will be locked out after three incorrect attempts at login.
- The user workstation will notify the user if a password does not meet the complexity requirements.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- **Users will be prompted when passwords must be changed.**
- Exceptions to any portion of this policy must be approved by the Senior Manager of Technical Services.
- In the event of a critical situation, the Senior Manager of Technical Services or a Senior Vice President can authorize password sharing for a temporary period of time.

PROCEDURE: The following are guidelines and/or procedures that must be adhered to in support of the policy statement and objective.

General Password Construction Guidelines

Passwords are used for various purposes at The Fund. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, and local router/switch logins.

Weak or poor password choices:

- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- The words "The Fund", "Orlando", "Florida" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit.
(e.g., secret1, 1secret)
- Strong passwords have the following characteristics:
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

Password Protection Standards

Do not use the same password for Fund accounts as for other non-Fund access (for example, personal ISP account, option trading, benefits, etc.). Whenever possible, don't use the same password for various Fund access needs. For example, select one password for mainframe access and a separate password for LAN systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share your Fund password with anyone, including managers, administrative assistants or secretaries. All passwords are to be treated as sensitive and personal information.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE.
The Fund's Help Desk will never ask for your password.
- Don't reveal a password in an email message.
- Don't reveal a password to your supervisor.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (for example, "my family name").
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members.
- Don't reveal a password to co-workers while on vacation.

If someone demands a password, refer them to this document or have them call your manager.

Do not use the "Remember Password" feature of applications (for example, Eudora, Outlook, and Netscape Messenger).

Again, do not write passwords and store them anywhere that is accessible in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

If an account or password is suspected to have been compromised, report the incident to PC Support and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by authorized personnel. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Application Administration Account Any account that is for the administration of an application (for example, Oracle base administrator, ISSU administrator.)

Revision History

Date of Revision	Update Made	Made By
2/6/03	Deleted references for o complexity requirements – these are TBD	Nick Patellis
9/22/03	Removed DRAFT from Header/Footer	Nick Patellis
9/22/03	Changed cover page to internal use only. Changed rev number to 1.5.	Nick Patellis
9/30/03	Added statement concerning exceptions to password policy requiring approval	Nick Patellis
4/13/04	Changed rev number to 1.6.	Nick Patellis
	Added complexity requirements.	Nick Patellis
8/2/04	Changed rev number to 2.0 to alleviate confusion.	Nick Patellis



**Attorneys' Title Insurance Fund, Inc.
POLICIES/PROCEDURES**

Subject: Computer Audit Policy	Effective Date: 08/02/04
--------------------------------	--------------------------

Authorized by: J. Calabrese

Title: VP, Information Services

New/Revised: New

PURPOSE: To provide the authority for authorized personnel to conduct a security audit on any system at The Fund. The Fund has two types of audits: Technical and User.

Technical audits are performed to insure the security of system resources at The Fund and are directed at non-user specific information. Technical audits may be conducted to:

- Ensure the security strength of the system wide infrastructure.
- Investigate possible attacks against Fund assets.
- Develop strategic security plans for Fund assets.

User audits are directed towards individual or groups of users. User audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources.
- Investigate possible security incidents and ensure conformance to The Fund's Computer Acceptable Use policy.
- Monitor user activity where appropriate.

POLICY: This policy covers all computer and communication devices owned or operated by The Fund. This policy also covers any computer and communications device that are present on The Fund's premises, but which may not be owned or operated by The Fund, for example, vendor PCs, contractor PCs.

All systems must be open to auditing by appropriate individuals to insure compliance with applicable security policies. This document will outline The Fund's policy concerning audits.

When requested, and for the purpose of performing an audit, any access needed will be provided to authorized personnel. Determination of the need for an audit will depend on the type of audit required. Personnel are expressly prohibited from performing audits without authorization by one of the following individuals:

- Technical Audits – Technical Support Manager or Senior Vice President of IS
- User Audits – Senior Vice President for Employee Services

Access to the required resources will also depend on the type of audit.

Technical Audits

- Unlimited access to the resource(s) being audited will be granted.
- Administrator access will be provided to auditing personnel.

User Audits

- User level and/or system level access to any computing or communications device.
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted, or stored on Fund equipment or premises.
- Access to work areas (labs, offices, cubicles, storage areas, etc.).
- Access to interactively monitor and log traffic on Fund networks.

It is policy of Attorney's Title Insurance Fund, Inc. that ALL Internet communications, email, and web/ftp/messaging/streaming will be monitored and logged at all times. **Therefore, there is no right to privacy on any Fund computer system or system operating on Fund property.**

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Violation of this policy could include activities such as unauthorized monitoring or network traffic, unauthorized auditing of a user workstation, unauthorized viewing of a user workstation contents, etc. Additional violations could include the refusal of a system administration (Technical Audit) or a user (User Audit) to fully comply with the audit team's access to information as outlined previously in this document.



Attorneys' Title Insurance Fund, Inc.
POLICIES/PROCEDURES

Subject: User Account Creation and Deletion Policy	Effective Date: 06/01/05
----------------------------------------------------	--------------------------

Authorized by: J. Calabrese Title: VP, Information Services New/Revised: New

PURPOSE: To provide The Fund's policy on how systems accounts are requested and how accounts are removed.

POLICY: This policy covers all computers owned or operated by The Fund. The term "user account" includes: Windows logins, network accounts, and mainframe accounts.

Account Creation

All users will have a unique system account.

Managers and supervisors must submit a STARS request to create an account.

Employee Termination

Employee Services will handle the account deletion process once an employee is terminated or leaves the company.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.



**Attorneys' Title Insurance Fund, Inc.
POLICIES/PROCEDURES**

Subject: Software Audit/Inventory Policy	Effective Date: 08/08/03
------------------------------------------	--------------------------

Authorized by: J. Calabrese Title: VP, Information Services New/Revised: New

PURPOSE: To provide The Fund's policy on how to ensure licensing compliance with Microsoft's Enterprise Agreement for all workstations and servers running software programs or using client access licenses for the software listed herein.

POLICY: This policy covers all computers owned or operated by The Fund. The term "user account" includes: Windows logins, network accounts, and mainframe accounts.

To ensure licensing compliance with Microsoft's Enterprise Agreement including the following products:

- Windows Workstation (3.1, 3.11, '95, '98, ME, NT3.51, NT 4.0, 2000, XP)
- Windows Server NT, 2000, 2003
- Windows Advanced Server NT, 2000, 2003
- MS Office (including any of the following: Word, Excel, PowerPoint, Access, Outlook)
- MSDN Universal Win32 SA
- Project Pro
- Project CAL
- Project Server
- Visio Pro
- Visio Standard
- Exchange Server Enterprise
- SQL Sever Standard Edition
- SQL Sever Standard Edition Processor License
- System Management Server Enterprise Edition
- Windows Terminal Server Client Access License's

The following procedure must be adhered to in support of the purpose statement and scope.

Physical Inventories

1. Every March and September, Support Services will perform an inventory of PCs and Servers at The Fund. This inventory is to be completed and submitted no later than on the last working day of the month in which it was begun. The September inventory will consist of collecting asset tag numbers from each individual PC and End User names from an ATIF inventory sheet (see appendix A) or keying each number and name into a database. The March inventory will also include a physical audit of the listed software on each PC. In the case of servers, the name of the server will be captured indicating its physical location. The inventories of servers and PCs will be completed at the same time but are to be compiled separately. The end product of the inventory will consist of two spreadsheets. One will total the number of PCs indicating which listed Microsoft software is running on them (for the March inventory only) and one totaling the number of file servers and their locations. A server with a VM designation (this will be clearly marked on the front of the server) has more than one host. As such, this kind of server is a special case, and Support Services will work with Technical Services to determine the total number of virtual servers running on each of these servers for an accurate license count.
2. If these inventories are unable to be completed in the designated time, then a written explanation must be provided to the Support Services Manager. The Support Services Manager is then to report the reason to the Technical Support Manager.
3. Asset numbers are to be collected and grouped by location. For example, if a collector begins at Headquarters in Policy Operations, he must collect all the data in that location before moving onto the next location.
4. If any branch or data center is not in a Technical Services Hardware/Software Inventory database, then the inventory data that was physically collected and keyed into the spreadsheet will be considered the final and true inventory for that location.
5. ATIF Inventory sheets (or the format of the inventory collection sheets if a laptop or barcode scanner is used) are to be used in the collection of this data. A sample of these sheets is provided at the end of this document.
6. The data, once collected, is to be keyed into a spreadsheet by Support Services.
7. For the March inventory, Support Services will annotate the spreadsheet indicating which of the PCs use Microsoft software components (Word, Excel, PowerPoint, Access, Visio, or Project) and which are devoid of these components. If any PC has any one of these components then that PC will be said to be an "office automation" PC and so annotated on the spreadsheet. The PCs that have no MS Office components, or Project or Visio, will be so annotated on the spreadsheet as "Line of Business." Please see the sample spreadsheet in Appendix A.
8. When the spreadsheets have been completed, technical services will be notified via e-mail and the asset numbers reconciled to the technical services hardware/software inventory database.

9. When the data collection is completed and the spreadsheets are updated and have been reconciled to the Technical Services database, the final numbers will be e-mailed to the Branch and/or Data Center Managers, Distributed Systems Supervisor, and the Support Services Supervisor.
10. These numbers will be used as a count to compare what is currently owned in Microsoft products vs. the number of Microsoft product licenses owned. These numbers will be used to "True-Up" the Microsoft enterprise agreement that is currently in place.

Reconciliation of Data

Data is to be reconciled by technical services against the technical services hardware/software inventory database.

The assigned technical services administrator will run software inventory reports displaying what software is running on each PC.

The assigned technical services administrator is to rely on the compiled physical inventories and the data available from the databases to come to consensus on the number of PC's and servers at The Fund and the type of software being run on these machines.

This compiled data is to be delivered in the form of:

- Number of PC's
- Number of PC's running Visio
- Number of PC's running Visio Pro
- Number of PC's running Project
- Number of PC's running Project Pro
- Number of PC's running Microsoft Office
- Total Number of Office Automation PC's
- Number of PC's not running Office, Project or Visio.
- Total Number of Line of Business PC's
- Total Number of Servers and the OS version of software running on each server

The Distributed Systems Supervisor will use this as the "official count."

The Distributed Systems Supervisor will supply the current-licenses-owned count and the current-license-in-use count to the Technical Services Manager. The Distributed Systems Supervisor will also supply the counts to the Support Services Supervisor who will insure we are in compliance with our Microsoft licensing agreement.

All effort will be made to eliminate old PC's through retirement and attrition. The focus of this effort will be to keep our total EA license count as low as possible. This will help eliminate the need to purchase additional EA licenses in the future.

Appendix A

ATIF PC Inventory Sheet								
Office:	Broward							
Department:								
Floor:								
PC Asset Tag	User	Office	Project	Project Pro	Visio	Visio Pro	Office Automation	Line of Business
L0004186	John Doe	Y					Y	N
L0004189	Jane Doe	Y	Y			Y	Y	N
L0004250	Jim Smith						N	Y

ATIF Server Inventory Sheet	
Server Name	Location
ORLFS1	HQ
DADFS1	Dade
DADPS1	Dade



Attorneys' Title Insurance Fund, Inc.
Policies and Procedures

Subject: Project Change Management Process	Effective Date: 10/01/2004
--------------------------------------------	----------------------------

Authorized by: J. Calabrese Title: SVP, Information Services New/Revised: New

Purpose: All changes to IS projects that meet the criteria below must use the Project Change Request (PCR) process.

Policy: The purpose of the Project Change Management policy is to control project scope by documenting all changes to budget, schedule and/or functionality of all Strategic, Infrastructure and projects introduced by the Business Oversight Board. The change document formalizes the information gathered surrounding the change and provides a method for the Project Sponsors and Business Oversight Board (BOB) to review and determine disposition.

Procedure

All changes to the baseline scope, schedule or budget for strategic, infrastructure, or projects introduced by the Business Oversight Board, are submitted to the Project Lead for analysis and approval.

The Project Lead will assess the impact to the project. The assessment is documented on the attached Project Change Request (PCR) Form. The change should be reviewed with the responsible Product Manager and the Resource-owning Manager (when applicable).

The PCR and relevant supporting documentation is sent to the PMO representative to review any impacts to the IS Master Plan and resource allocation. The PCR is assigned a number (format is project code followed by a sequential number) and any relevant impacts are documented on the PCR.

The PCR form is submitted to the Project Sponsor for review and first level approval.

- If the change is less than one FTE month in total effort (analysis, coding, testing), and can be accommodated in the project schedule without impacting other projects or the budget (by an increase of 5% or \$10,000, whichever is greater) and if the Project Sponsor approves the PCR, then it is incorporated in the project plan.
- If the change impacts the IS Master Plan or approved project budget (by more than 5% or \$10,000, whichever is greater), the document is submitted to BOB for review and final approval.
- If the magnitude of the change is significant (greater than \$100,000), then BOB will submit the PCR to EMT for final approval.
- If the PCR is approved, the change status is updated to "Approved," and the project plan is updated (including all relevant documentation including the schedule, scope, requirements use cases etc), and the Master Plan and Resource Allocations are updated as well.

- If the PCR is rejected: (Either by the Sponsor, BOB or EMT) the change status is updated to “Rejected.”

Final disposition is documented on the PCR by the Project Lead and communicated to the originator by BOB and the Project Lead.

The originator may appeal a decision directly to EMT. The disposition of the appeal should be communicated to BOB and the Project Lead by the PMO.

Exceptions

- Changes for operational or sustaining projects will follow the Policy Project Change Management – Operational.
- If the change is critical and requires an immediate decision, a “Fast-Track” Approval Process can be used to expedite the decision, but the PCR form must be used.
- A PCR is not required if the project has not completed their formal design review or does not have an approved project plan.
- **A PCR does not require Sponsor approval if it does not impact the baseline end of phase milestones or completion dates.**
- If the change is less than \$10,000 or 5% (whichever is less) of the total project budget and does not extend the schedule as follows:
 - Changes identified during the Construction phase and do not impact the schedule by more than one month.
 - Changes identified during the Transition phase and do not impact the schedule by more than one week.
 - Changes to a project that are a result of another change request do not need to be documented and approved. The impact to other projects is considered in the original change request.

Specific Requirements

- A Project Change Form is required for all changes. The exceptions listed in section 2 do not require formal approval.
- Impacts to other projects must be considered in the change request.
- Changes that affect the Business Case should be documented and sent to the Project Sponsor, Financial Analyst and the Productivity and Member Services Manager (Employee Services) for review and approval.
- Approval to move forward is required by the Project Sponsor and if the change cannot be absorbed in the existing plan, BOB and/or EMT.
- All affected project plans are updated appropriately by the Project Leads and PMO.
- Changes are communicated to all affected parties by the PMO (if the change request went to BOB or EMT) or the Project Lead (if the change request went to the Sponsor level only).

Project Change Request Form

Activity Code: Assigned by Finance	Project Name:	Request Date:	
Change Number: Assigned by PMO	Requestor Name:	Date Needed:	
Prepared by:	Project Lead Name:	Change Type: Schedule, budget or scope	
Description of Change: Brief description of the change			
Value or Benefit: Why does the business need this change? What are the quantifiable benefits?			
Impact on Scope and/or Deliverables:			
Cost	Increase by: Support with detail attached.	Decrease by: Support with detail attached	
Schedule	Increase by: Support with schedule – list duration	Decrease by: Support with schedule – list duration	
Scope	Increase by: Support with revised scope – highlight here	Decrease by: Support with revised scope – highlight here	
Quality	Increase by: If change will affect quality	Decrease by: If change will affect quality	
Alternatives if Change is not Approved: Does a work-around exist?			
Impact if Change is not Approved: What happens to the business partner if the change is not approved? What is the cost of the work-around?			
Impact(s) to Other Projects: List the projects that are impacted. Resources? How much are they impacted?			
Disposition of Change Resolution:		Accepted:	Denied:
Signature of Project Lead:		Date:	
Signature of Product Manager responsible for project:		Date:	
Signature of Project Sponsor:		Date:	
Signature of Project BOB Representative:		Date:	

Subject: Methodology	Effective Date: 06/01/1998
----------------------	----------------------------

Authorized by: J. H. Clark

Title: SVP, Information Services

New/Revised: Revised

Purpose: Methodology provides an organizational framework for project development by defining the roles and responsibilities of all those involved in a project, as well as establishing standards for tasks to be done. By clearly defining the tasks to be done, methodology provides the basis for training that will improve leadership skills and increase the likelihood of project success. This process promotes communication, planning, and control. For further reference regarding Methodology standards and guidelines, refer to the Methodology Guidebook and Procedures.

Policy: It is the policy of Information Services to use a formalized approach to project development and implementation. This approach will ensure the timely and cost effective production of products, maintain acceptable standards of quality, and achieve the benefit for which the project investment has been made.



Attorneys' Title Insurance Fund, Inc.
POLICIES/PROCEDURES

Subject: Electronic Mail Use	Effective Date: 04/01/99
------------------------------	--------------------------

Authorized by: J. H. Clark Title: SVP, Information Services New/Revised: Revised 02/18/03

Policy: It is the policy of The Fund to ensure the availability of the corporate Electronic Mail (email) system to its users. The Fund's email system is a business communications tool and should only be used for business purposes. The Fund reserves the right to access, monitor, record, or copy any email messages sent or received by a Fund employee or agent, with or without notice.

Procedure: To gain access to Internet email, the attached Internet Access Application Form must be completed. This form requires the signature of the responsible area manager and the approval by Information Services. Once this form is completed, it is forwarded to Technical Support for action. Technical Support will add users once a week in bulk. Once a user is added, the user is presented with a copy of this policy. The user must read the policy and sign the attached letter of understanding.

- Attachments should include graphics **ONLY** when absolutely necessary, since graphics greatly increase the size of the message and the space on our email server.
- Broadcast messages should not be sent to everyone in the mail address listing. Messages should only be sent to the list of appropriate individuals. Exceptions are notifications of email downtime or other events that will affect all users.
- A storage limit on the mail server of five (5) megabytes for local users and four (4) megabytes for mobile users will be imposed, unless otherwise approved by management. Laptop users have unlimited storage of email to the C:\Drive. Management may request additional space by submitting a STARS request.
- The default color combination of black text on white background is the approved standard. Other colors should be used only for highlighting and emphasis.
- Access to Internet email will be allowed only upon initial approval by the employee's manager and upon final review and approval by Information Services.
- Upgrades to the email client software by the individual user **are not allowed**.
- The email system should not be used for the delivery of urgent telephone messages. Because some users do not regularly check their email, the preferred delivery means for urgent messages is always via some form of personal contact.
- Email is a written, not oral, communication tool and must be regarded as such. Harsh or derogatory language, inappropriate off-the-cuff remarks and the like should be avoided. Users are advised not to include in an email message any language that would be ill advised or inappropriate in a written memorandum or

correspondence. Once an email is delivered, it is considered permanent. Email is retained in the system indefinitely on backup tapes.

- Use of email should be avoided for “chain” messages that continue over an extended period of time and have a number of people responding back and forth. In these cases, participants should decide to get together either personally or via conference call to bring all issues to a speedy resolution.
- In responding to meeting requests, individual respondents should reply **ONLY** to the person setting up the meeting and not use the “Reply to All” feature. This avoids needless clutter to the mailboxes of the other invitees. The meeting organizer can deal with all correspondence to the other invitees.
- Correspondence containing sensitive information may not be sent via the email system unless password-protected.
- All attachments received from the Internet should be saved to disk and scanned for virus corruption before opening.
- All messages will use the “NORMAL” setting of *Importance* and *Sensitivity* unless absolutely necessary. Matters of high urgency should be communicated personally.
- Internet email “SPAM” is a serious issue. SPAM is unsolicited commercial email including the introduction of questionable products and services, get-rich-quick schemes, dial-a-porn, and other undesirable offerings. The user is prohibited from responding to such offerings. Users should notify Technical Support for assistance in dealing with this issue.
- The Fund has inbound email filtering in place to stop SPAM (unwanted or junk email). The system uses several factors to determine whether an email should be dropped, including:

Originating email address	If an email address is from a known SPAM website, it will be blocked
Subject Line	There is a list of inappropriate words and phrases which if contained in the subject or body of the email will cause the email to be rejected.
Content of the email	There is a list of inappropriate words and phrases which if contained in the subject or body of the email will cause the email to be rejected. Additionally, HTML email will also be blocked.
Attachments to the email	Only .doc, .xls, .zip and .pdf files are permitted through our email filter system.

- All mail and attachments will be scanned for viruses and for violation of content filter rules. Messages that violate content filter rules and virus contaminated messages will be quarantined and/or deleted.
- The Internet is a public network; users cannot expect that any information transmitted over the Internet will be kept private. Employees should therefore not post personal comments or opinions to, or over, the Internet, or use the Internet for personal reasons without obtaining prior authorization from the user's manager. In cases where such authorization is granted, users may be required to include a disclaimer indicating that their comments and opinions are their own and do not represent The Fund's (for example, "The comments and opinions expressed are my own and do not represent the views of Attorneys' Title Insurance Fund, Inc.")
- The responsibility for general mailbox housekeeping falls to the user. These housekeeping duties include the following:
 1. Delete messages that are not needed on a daily basis.
 2. Move all messages that need to be saved to a personal folder.
 3. Do not activate or use the Journal folder.
 4. Empty the Deleted Items folder regularly.
 5. Review the Sent Items folder regularly. If items need to be saved, move them to a personal folder.
 6. When the system prompts the user for archival activation, accept the query.
- Violations of this policy will be subject to appropriate disciplinary action under The Fund's Policies and Procedures. In addition to disciplinary action, a violation may result in denial of email access to the employee.
- Additional information related to Internet and Email usage can be found in The Fund's Computer Acceptable Use Policy.



Attorneys' Title Insurance Fund, Inc.
POLICIES/PROCEDURES

Subject: How to Share Email Inboxes	Effective Date: 08/15/03
--------------------------------------------	---------------------------------

Authorized by: J. H. Clark Title: SVP, Information Services New/Revised: New

Policy: It is the policy of The Fund to ensure a manager has the capability to access an employee's email inbox. The Fund's email system is a business communications tool and should only be used for business purposes. The Fund reserves the right to access, monitor, record, or copy any email message sent or received by a Fund employee or agent, with or without notice.

Purpose: To allow the sharing of email inboxes.

Procedure: To allow a manager to view an employee email inbox, the manager must authorize the access. Outlook calls this access process Delegation. The process for granting Delegation requires two steps: one on the employee's PC, and one on the manager's PC.

Employee's PC

1. The employee granting access to his manager clicks Tools > Options.
2. When the Options menu is displayed, the employee clicks Delegate.
3. To add his manager, the employee clicks Add. A list of all email users is displayed.
4. The employee selects the manager's name. A list of Delegate Permissions is displayed.
5. The employee selects Inbox and allows the manager to have Editor rights.
6. The employee clicks OK and clears all the menus.

Manager's PC

1. The manager granted permissions by his employee sets his or her Outlook to view the employee's inbox. To do so, the manager clicks File > Open > Other User's Folder.
2. The manager types the employee's name in the Open Other User's Folder window.
3. The employee's inbox is displayed.

The Delegation process does not allow the manager to create emails as the employee. However, using this process, the manager can:

- View the contents of the employee's inbox.
- Open and read emails.
- Reply to an email as the employee.
- Forward emails to the manager's email address or to that of another user.
- Delete email.

The manager need only create these settings a single time on his or her PC. Outlook retains the information concerning the employee's folder. To view the employee's inbox in the future, the manager clicks File > Open > (employee's name).



Attorneys' Title Insurance Fund, Inc.
POLICIES/PROCEDURES

Subject: Internet Usage Policy	Effective Date: 04/01/99
--------------------------------	--------------------------

Authorized by: J. Calabrese Title: SVP, Information Services Revised: 07/23/02

Purpose: The purpose of this policy is to outline Internet Usage at Attorneys' Title Insurance Fund, Inc. These rules are in place to protect the employee and The Fund. Inappropriate use of the Internet exposes The Fund to risks including virus attacks, compromise of network systems and services, and legal issues.

The use of the Internet is restricted to general purpose business activities and other such purposes that are expressly authorized by management. **Use of the Internet must also be in accordance with the Computer Acceptable Use Policy.**

Policy: This policy applies to employees, contractors, consultants, temporaries, and other workers at The Fund, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by The Fund.

- Users are not automatically granted Internet access. A user's manager must put in a STARS request for a user to be granted Internet access. Information Services (IS) reviews all requests for validity.
- All user activity on the Internet will be monitored. There is no right to privacy for any information to and from the user. **See the Computer Audit Policy for additional information.**
- All Internet software used by The Fund must be approved in advance by the Strategic Architecture Review Committee (SARC).
- No Freeware/Shareware shall be downloaded by any method, or installed on The Fund's computing resources by any employee other than by those technical employees specifically authorized by IS management.
- All downloaded files must be scanned for virus corruption before use. This includes, but is not limited to, text documents, spreadsheets, images, graphics, and software patches. Downloaded software may not be used in connection with the design, development, or manufacture of any product or the provision of any service by The Fund unless The Fund has first entered into a written license agreement with the software vendor.
- Copyrighted textual material may be downloaded if permitted by the material's copyright statements as long as the provisions of those statements are followed and in no way bind or obligate The Fund.
- Access to the Internet will be via The Fund's private network through a firewall. Desktop modem access to the Internet is prohibited unless specifically approved via a STARS request to Technical Support.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.



**Attorneys' Title Insurance Fund, Inc.
POLICIES/PROCEDURES**

Subject: Internet Web Content Policy	Effective Date: 05/01/02
---------------------------------------------	---------------------------------

Authorized by: J. Calabrese Title: SVP, Information Services New/Revised: New

Purpose: The purpose of this policy is to outline what is considered appropriate material to be published on any Fund website. This policy is in place to protect internal Fund documents, business practices, employee information, and other information deemed sensitive in nature.

Policy: The intention for publishing on an Internet Web Content Policy is to provide guidance for what is appropriate content to be published on the public Fund websites. This policy applies to all employees who publish web content on any approved Fund website.

Approved Content

- Any information that has been released publicly by The Fund.
- Any information that has been released via a news release.
- Information approved by the Senior Vice President of Marketing Services.
- Content developed through the Web Strategy Development Process as implemented by The Fund.

Non- Approved Content

- Personal information concerning any employee, such as social security numbers, employee home addresses, or phone numbers
- Information detailing internal operations of The Fund, such as building information, blueprints, or diagrams,
- Infrastructure information such as electrical, networking, Internet systems, and internal systems
- Internal application details
- Source code for any Fund application
- Internal employee phone list
- Proprietary business information
- Any information covered by a Non-Disclosure Agreement (NDA)

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.



**Attorneys' Title Insurance Fund, Inc.
POLICIES/PROCEDURES**

Subject: Telephone Usage Policy	Effective Date: 02/11/03
----------------------------------------	---------------------------------

Authorized by: J. Calabrese Title: SVP, Information Services New/Revised: New

Purpose: The purpose of this policy is to outline The Fund's policy on the use of telephone and fax systems. Telephone and fax systems are business assets that must be used correctly. This policy covers all telephone and fax equipment in use at any Fund facility and discusses the correct usage of these systems.

Policy: The Telephone equipment and lines subscribed to by The Fund are for the purpose of supporting the business goals and objectives of The Fund. The company may, on a periodic basis, view reports produced through the communication system to ensure the proper use of the telephone and fax machines.

Telephones are not to be used excessively for local personal use and may never be used for personal long distance phone calls that will be billed to The Fund. The (800) numbers are for business use only and may never be used for personal use.

Fax machines function through the telephone lines. Therefore, the same rules apply for the use of the fax machines. Employees may not receive or send personal information through the use of company fax machines that will result in an expense to The Fund. Again, this includes the use of company (800) numbers.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.



ATTORNEYS' TITLE INSURANCE FUND, INC.
POLICIES / PROCEDURES

5 F

Subject: Purchasing Information Technology

Effective Date: 9/1/06

Authorized by: J. Calabrese

Title: SVP, Information Services

New/Revised: New

Policy:

Purchases and lease arrangements for new Information Technologies shall be procured using a best value determination. This includes all purchases of hardware, software, technical consulting and technical services purchased within The Fund. All such procurements at ATIF shall also adhere with the *"Computer Hardware and Software Standards"* identified in Information Services Policies and Procedures – 2A.

Definition:

Best value means the optimum combination of economy and quality to achieve the objectives of the end user and ATIF as a whole. To determine the optimum combination, decisions must be made on the pre-purchase evaluation criteria pertaining to the specific purchase. There may be different guidelines for goods and services although IS purchases shall uphold ATIF technical standards. The criteria shall be pre-determined and may include some or all of the following examples: price, quality, service after the sale, conformity with infrastructure and platform standards, disruption costs, training, installation, and supplier financial health.

Purpose:

This is an ATIF-wide policy pertaining to technology purchases to insure new architectural components and services engagements are defined and obtained with consistent contractual terms and standards. The goal of this policy will be that all new information technology and services be purchased to a set of pre-defined criteria and be placed under contract using common terms, conditions, well-defined timelines, deliverables and standards.

Risks:

IT purchases of non-compliant components and providers increase the cost of operations. Deviation from the policy and procedures may result in weak definition of deliverables, disparity in contract terms, higher costs, conditions and remedies.



Procedures

When purchasing new information systems hardware, software and/or service(s), the following basic procedural tenets shall apply:

1. **Solicit:** Information Services and others as appropriate shall solicit the market using a pre-written set of requirements and establish selection criteria in advance of receiving responses. The best practice is to write a Request-For-Proposal (RFP) including our preferred contract terms and to release to a minimum of three potential providers.
2. **Assess:** Information Services and others as appropriate shall assess the potential providers' capabilities to fulfill the requirements and meet our preferred contract terms and conditions. Best practices are to research the product/service capabilities through RFP responses, on-site demos, site visits, technical proof-of-concepts, and reference checks and referrals. This does not preclude the use of sole-source providers although does suggest that the selection be defined in business terms. The Information Services representative purchasing the technology will prepare and submit a *"Technical Evaluation Document"* to the Technology Oversight Group for approval to procure the technology.
3. **Negotiate:** Information Services will firm the contract terms and conditions and select best value. Even for the purchase of commodities, it is valuable to shop around to find the best arrangement. For complex buys of services, the Vendor Manager will help develop contract terms and service agreements through a Professional Services Agreement and/or a Statement-of-Work to crisply define the deliverables, schedules and payment terms.
4. **Purchase:** All purchases of hardware, software and technical services will be obtained using a Purchase Order with the existing ATIF procedures defined by Finance. Once signed, all contracts and Statement-of-Works' shall be placed in ATIF Central Files with copy to Vendor Manager, IS Shared Services.
5. **Monitor:** The Information Services representative purchasing the Information Technology shall be responsible to insure all goods and services are fulfilled per the agreed contract terms. Information Services, through the Vendor Manager or other designee, may periodically audit the procedures and execution to insure ATIF's fulfillment and best interests are being maintained.



Attorneys' Title Insurance Fund, Inc.
POLICIES/PROCEDURES

Subject: Application Data Ownership Policy

Authorized by: Jeannie Calabrese Title: SVP, Information Services Created: 6/15/06

Purpose: All applications must consider the requirements of the ownership of the data they create.

Scope: All Fund applications both internally developed as well as COTS.

Policy: **Data Ownership Documentation**

Applications create and manipulate data which must be managed. Steps required in the management of this data are:

1. Determine who owns the data
2. Who has access to the data
3. What type of access a person has to the data
4. Who installs the controls on the data

In order to implement the four steps listed above, two roles are being developed:

Data Owner – Individual identified as the owner of the data. They are responsible for determining who has access to the data and the type of access each user will have to the data.

Custodian – The individual or group who implements the data owner's requirements for users requiring access and the access level they require. This role usually fulfilled by system or application.

Data Ownership Processes

Four process steps must be created for each application's data. These steps can be incorporated in application documentation in lieu of creating a separate process document.

Required processes to be defined for each application

1. Identification of users or groups of users who require access to the application data as well as data owner.
 - a. This must be to the group of users level, i.e. General Ledger
 - b. The data owner must be identified by position with an alternate, i.e. Comptroller and Assistant Comptroller
2. How requests for individual or group access is completed as well as removal of individuals or groups access to the data. In order to track the changes required, STARS is the preferred method. The team that is creating the application must include in their requirements the exact methodology STARS will be using. It is the responsibility of the data owner, or their designee to complete the STARS request for addition or removal of an employee.
3. Specific rights each group requiring access will require
 - a. Read
 - b. Write
 - c. Delete
4. The data owner must understand they are responsible for reviewing at least yearly all groups and users who have access to their data.

When an employee transfers positions, the manager/supervisor who is losing the employee must ensure the employee's access to their data is also revoked. The gaining manager/supervisor will grant new access requirements.

Both of these requests will require STARS requests. The losing manager/supervisor will submit a request to remove the employee access and the gaining manager/supervisor will submit a request to add the employee access.