ACTION TITLE SERVICES
of St. Johns County, Inc.

Our Security Policy

Our Security Statement

Action Title Services of St. Johns County, Inc. has taken measures to guard against unauthorized or unlawful processing of personal data and against accidental loss, destruction or damage.

This includes:

- Adopting an information security policy (this document is our policy).
- Taking steps to control physical security (projects and staff records are all kept in a locked filing cabinet).
- Putting in place controls on access to information (password protection on files and server access).
- Establishing a business continuity/disaster recovery plan (including, at a minimum taking regular back-ups of its computer data files and this is stored away from the office at a safe location).
- Training all staff on security systems and procedures.
- Detecting and investigating breaches of security should they occur.

Basic Principles

1. Personal data is to be collected only for the purpose specified.
2. Data collected is to be relevant but not excessive for the purposes required.
    a. On an annual basis, title insurance application forms and any other forms that we use are reviewed to confirm that we are not asking for irrelevant information
3. Data is not to be kept for longer than is necessary for the purposes collected, including complying with applicable laws. Within 60-90 days of closing:
    a. Files are scanned into our secure server and paper copies are shredded
    b. Files are moved to locked files in a secure location in our office
4. We protect the data with appropriate technical and organizational measures to minimize the risk of unauthorized or unlawful processing and against accidental loss or destruction or damage to personal data.
    a. Servers are stored in locked facilities with access limited to: management and business owners.
    b. Remote access to files is not available.
    c. The servers and computers are disconnected from the internet during non-business hours.
    d. Annual Testing for External Penetration to try to hack in – which is done by an outside company.

5. Data is not removed from the office, except when contained on/within appropriately secured data transmission methods.
    a. Paper files are never removed from the office except as needed for a remote closing.
    b. Remote access is not provided to our server for employees.
    c. Company does have acceptable I.T. Computer Use Policy that each employee has read and acknowledged by signature on an annual basis.
6. Access to data whether current or archived is provided to those individuals who, in the course of performing their responsibilities.
7. All data on the network is protected by Sonic Wall anti-virus software that runs on servers and workstations, and is updated automatically with on-line downloads from the Sonic Wall website / via updates received on CD. This includes alerts whenever a virus is detected.
8. Any viral infection that is not immediately dealt with by Sonic Wall is notified to the Agency Owner.
9. All user data is backed up to Carbonite automatically on a daily basis, using an appropriately secure system for fast indexing and data restoration.
10. A full server backup to Carbonite takes place nightly.
11. A separate business continuity plan is also established.
12. Company also adheres to a Clean Desk Policy.
13. Company has posted their Privacy Statement on their website.
14. Company uses Encryption to transmit any NPI

ACTION TITLE SERVICES
of St. Johns County, Inc.

Our Technology Policy

Purpose of Information Technology Company Policy

This policy covers the access to Information Technology (IT) assets, including but not limited to network and applications, owned or operated by **Action Title Services of St. Johns County, Inc. (ATS)**.

Application of Policy

This policy applies to all **ATS Company** employees, affiliates, contractors, and vendors.

Information Technology Company Policy

The company shall establish processes to properly control access to the information technology assets. Access to information assets is to be controlled through a managed process that addresses authorizing, modifying, revoking, and periodic review of access privileges to all of the company's technology systems. This company policy provides the minimum requirements for authorizing and authenticating users prior to granting them access to information technology assets.

1) **Roles and Responsibilities**
    a) Managers are responsible for reviewing and approving all requests for access to the information assets for all users under their supervision, including modification of access rights.
    b) Managers are responsible for reporting changes in user duties or employment status for all employees under their supervision to the IT department.
    c) The IT department is responsible for granting the level of access that has been approved by the Business Manager.
    d) The IT department is responsible for maintaining record of the access requests in compliance with the Access Control Standard. This includes roles, and access modification, and termination.
    e) Only administrators explicitly authorized to create new accounts may create new users and user groups.
    f) Third parties given access are bound under a non-disclosure or other binding agreement of confidentiality that includes restrictions on the subsequent dissemination and usage of the information and defines the terms and conditions of such access.
2) **User Enrollment and Authorization**
    a) ATS's Enrollment Process establishes a user's identity and anticipated business needs to information and related information technology assets prior to granting user access to

the Company network and systems. The user is granted access to various information assets of the Company once the network user identification is assigned.

b) For all Company employees, contractors or service providers that require access to a Company information asset, a New User request must be submitted by the appropriate requestor (i.e. HR).
c) The New User request must indicate the IT assets to which the user would need access and the level of access.
d) The New User request must be approved by the appropriate approver (i.e. new employee supervisor) before being transmitted for execution to the IT department.
e) The IT department will grant access to the Company information assets as indicated on the previously approved request.

3) User Rights Modification

a) A request shall be submitted by the appropriate requestor (i.e. the employee requesting access) for each modification to a user's access rights.
b) The user rights modification request should indicate the IT assets to which the user will need access.
c) The request must be approved by the appropriate approver (i.e. employee's supervisor) before being transmitted for execution to the IT department.
d) The IT department grants access to the Company information assets as indicated on the approved request.

4) User Access Termination

a) Managers are responsible for communicating user access termination for all users under their supervision to the IT department.
b) The access termination communication must indicate the IT assets to which the user had access.
c) The Access termination communication must be submitted by the end of the last day worked by the user to HR & IT.
d) User access privileges for terminated employees must be performed in compliance with the Company's Access Control Standard.
e) In case of a high-level employee termination, the employee's supervisor must immediately coordinate the disabling of all the accounts for that employee.

5) Review of User Access Rights

a) Managers are responsible for reviewing the access rights for all users under their supervision to determine if access rights are commensurate to the users' job duties.
b) User Access Rights Review should be performed and documented at least as often as defined in the Company's Access Control Standard.
c) Evidence of account reviews shall be maintained in compliance with the Company's Access Control Standard.

6) Inactive Accounts

a) Review of accounts for general users shall occur in compliance with the Company's Access Control Standard to identify unused or inactive accounts.
b) Accounts that have not been used for a period of time (30-90 days), as defined in the Company's Access Control Standard, will be automatically disabled.

7) Identification

a) User IDs must be associated with the individual user to whom they have been assigned.
b) To minimize the risk that dormant access permissions accidentally being inherited by a new user, there should be **no re-use of any User IDs**.

c) User IDs are not to be utilized by anyone except the individual to whom the IDs have been issued. **No shared IDs!**
d) Users are responsible for all activity performed with their personal User IDs.
e) All users with access to the Company's information assets are to use a User ID that has been specifically assigned to them. **No shared IDs!**

8) Password Requirements

a) Access to ATS's computers, applications, and systems must be protected by passwords to prevent unauthorized use, following the Access Control Standard.
b) There are change parameters in place.

9) Password Protection Requirements

These requirements apply to both user and service accounts.

a) The password for ATS's accounts are not for other non- ATS access (e.g., personal ISP account, option trading, benefits, etc.).
b) ATS passwords are not shared with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential information.
c) If someone demands a password, we refer them to this document or have them call someone in the Information Security Office (IT).
d) The "Remember Password" feature of applications is not used unless the credentials are stored encrypted.
e) Passwords are not be stored in a file on ANY computer system without encryption.
f) If the compromise of an account or password is suspected, the incident must be reported to the Information Security Office and all passwords are changed immediately.
g) The ISO or its delegates may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it.

10) Authentication

a) Authentication methods will be consistent with the level of sensitivity of the information that the system in question contains.
b) At a minimum, a username and password are required.
c) Appropriate authentication controls are required when accessing internal system resources from outside the ATS network.
d) All passwords, pass codes, access control devices, keys, security passes/badges, personal identification numbers and the like (collectively, "Keys") issued for the purpose of accessing ATS Company premises or Systems are the property of ATS Company.
e) The use any Key to access, store or retrieve any Company information is not permitted unless (i) specifically authorized in a particular instance or (ii) authorized in advance as to the type of Company information and Key to be used.

11) Privileged Account Access

a) Administrator accounts are only used to perform administration duties.
b) All users that have access to privileged accounts have their own personal accounts for normal business use.
c) Users with access to super-user or privileged accounts use their normal account to log into information resources for day-to-day use.
d) Privileged Account passwords are updated immediately after the dismissal of any employee who had access to administrator-level or privileged accounts.

e) Any combination of special privileges which could grant inappropriate privileges when combined (e.g., system administration and auditing) are segregated among different users to ensure proper segregation of duties.
f) Privileged accounts not associated with an individual are approved, documented and strictly limited to those with a business justification for use.
g) Persons with administrative rights always lock or log out of any active session prior to leaving the device unattended.

12) Service Account Password Requirements

a) Service Account passwords comply with the ATS Company Access Control Standard.
b) Changed on a regular basis.

13) Internet-Facing Web Application Password Requirements

a) Passwords in this category comply with the ATS Company Access Control Standard.
b) Changed on a regular basis.

14) Database Credential Requirements

a) Storage of Data Base Usernames and Passwords comply with the ATS Company Access Control Standard.
b) Retrieval of Database Usernames and Passwords comply with the ATS Company Access Control Standard.
c) Access to Database Usernames and Passwords comply with the ATS Company Access Control Standard.

15) Temporary Employees

a) Temporary employees will be issued individual accounts with passwords that automatically expire after a predetermined date.
b) When we set up temporary employees, the length of their employment will be identified, not to exceed the maximum temporary employee employment length defined in the ATS Company Access Control Standard.
c) Access is reviewed at the end of a temporary employee's employment.
d) If the employee's employment will not continue, the access to all systems must be removed.

16) Enforcement

a) Any employee found to have violated this policy will be subject to disciplinary action, up to and including termination of employment.
b) External service providers found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

ACTION TITLE SERVICES
of St. Johns County, Inc.

Our Record Retention and Record Disposal Policy

Action Title Services of St. Johns County, Inc. (ATS) is establishing its Record Retention Policy ("RRP").

This Policy is so important that every ATS Employee at every level must learn and observe its requirements. Compliance with the RRP is an important part of every Employee's daily responsibilities and is mandatory for every Employee with respect to that Employee's work as an employee of the ATS Company and its 3rd Party Vendors.

This Policy has three broad goals:

1) To make sure that ATS maintains its Records in the ordinary course of business in compliance with legal and business requirements.
    a) This means that Records are protected against deliberate or accidental destruction for as long as ATS needs to retain them by law and for business requirements; that the correct version of each Official Record is retained and kept only in authorized locations; that Records are retained only as long as ATS is required to keep them (in accordance with the appropriate Record Retention Schedule or in compliance with a Legal Hold Order issued by Management); and that Records are retired in a suitable way at the end of their retention period, unless such Records are subject to a Legal Hold Order.
2) To ensure Legal Hold Orders are issued, when necessary, and enforced.
    a) Legal Hold Orders are orders to ATS Employees and 3rd Party Vendors to preserve Records that relate to current or reasonably anticipated litigations, government investigations, subpoenas or claims. Compliance with a Legal Hold Order is critical. Every Employee must understand how to respond to a Legal Hold Order if he or she receives one.
3) To be sure that Company Information is treated as confidential information and is always protected against unauthorized disclosure.
    a) Records may contain Company Information, which should be kept as confidential information. Some of the **Company Information may be non- public personal information** that, if disclosed, could enable identity theft.

b) Such non-public, personal information and ATS's Trade Secrets must always remain confidential. It is essential that confidentiality requirements are always observed, even after an Employee leaves ATS.
c) Preserving the confidentiality of Company Information means protecting it from intrusion by people outside the Company, as well as by people inside ATS who are not authorized to see that Company Information. It also means making sure that when Records containing Company Information are retired, the retirement is handled properly and securely: (i) Company Information containing ATS's Trade Secrets, non-public personal information of past, present or potential customers or Employees (such as social security numbers, health information, credit card information and the like) should be destroyed so that it cannot be read or reconstructed and (ii) all other Company Information should be destroyed in accordance with the Company's practices applicable to such information.
d) Records fall into one of two classes: Official Records and Convenience Records **defined as**:

"**Official Records**" are Records that must be kept for specific periods of time to meet legal and business requirements. Examples of Official Records include tax records or HR records. Official Records are listed on the appropriate Record Retention Schedule, along with the period of time they need to be kept. After that time, they are routinely retired (unless subject to a Legal Hold Order).

"**Convenience Records**" are Records that have no retention requirement unless they are subject to a Legal Hold Order. Convenience Records include working copies, drafts of Official Records, notes, telephone messages and similar items. Convenience Records may also include information that you generate or receive and does not pertain to ATS business (such as personal e-mails, calendars or notes), but that is stored on ATS technological property. Convenience Records can be discarded when we no longer need them (unless they are subject to a Legal Hold Order).

As between ATS Employees or 3rd Party Vendors and ATS, Records are the property of ATS and subject to its control. Such control shall be exercised over the creation, distribution, utilization, retention, storage, retrieval, protection, preservation and final disposition of these Records.

1. Definitions.

a. "**Company**" or "ATS" means ATS Company.
b. "**Company Information**" means all materials or information in whatever form, whether written, oral, digital or otherwise that is (a) defined as "confidential" or is a Trade Secret hereunder or under any ATS policy or under any agreement to which ATS is a party; (b) subject to special protections that require confidentiality under any law or regulation; (c) non-public and that relates to ATS's finances, Employees (whether past, present or potential), research, development, facilities or business or (d) non-public personal information relating to a past, present or potential customer of ATS that identifies the customer in any way (including information that is publicly available, but whose disclosure would indicate that ATS had a customer relationship with that individual).
c. "**Convenience Record**" means a **Record** that has no retention requirement and that may be retired at any time unless it is subject to a Legal Hold Order. Convenience Records include working copies, drafts of Official Records, notes, telephone messages and similar items. Convenience Records may also include Employee generated or received information that does not pertain to ATS business (such as personal e- mails, calendars or notes), but that is stored on ATS's technological property.

d. "**Corporate Record Retention Officer**" is a member of the Company's Record Retention Committee with special duties, which are set forth in Section 4(b) below.
e. "**Employee**" means every person employed by ATS at any level.
f. "**Legal Hold Officer**" is a member of the ATS's Legal Department or Management Group (designated by the Company) with special duties related to Legal Hold Orders, which duties are set forth in Section 4(e) below and in the ATS Legal Hold Order Procedure.
g. "**Legal Hold Order**" means a direction to preserve and to prevent the destruction of Records that may be required for a pending or reasonably anticipated litigation, government investigation, subpoena or claim. As a general matter, a Legal Hold Order issued pursuant to the ATS's Legal Hold Order Procedure does not apply to the litigation of insurance claims or policies issued by ATS or to tax disputes (such litigation and disputes are subject to other ATS practices to preserve and to prevent the destruction of relevant Records).
h. "**Legal Hold Order ID Number**" is a number that will be assigned to each Legal Hold Order by the Legal Hold Officer and will be included on all documentation (e.g., communications sent to potential custodians, data users, records managers, IT personnel, Listed Vendors, etc.) related to the Legal Hold Order.
i. "**Legal Hold Team**" means the group of individuals with duties related to Legal Hold Orders, which duties are set forth in Section 4(d) below.
j. "**Listed Vendor**" means any third-party service provider of ATS that either controls or has access to Records and is listed on the Vendor List on the Record Retention Website.
k. "**Litigation Counsel**" means the attorney with ultimate responsibility for the particular litigation or investigation in question.
l. "**Record Retention Officer**" is a person at ATS responsible for answering questions with respect to the Program and who reports on such matters to the Corporate Record Retention Officer, as set forth in Section 4(c) below.
m. "**Official Record**" means a Record that must be kept for a specific period of time (identified in the Record Retention Schedules) to meet legal and business requirements.
n. "**Record**" means any information under ATS's control that relates to ATS's business; finances; past, present or potential customers and Employees; operations; research and development; and facilities. Records fall into one of two classes: Official Records and Convenience Records.
o. "**Record Retention Committee**" means a permanent committee of representatives drawn from the Legal, Regulatory, Compliance and IT departments at ATS with duties related to oversight of the Program, which duties are set forth in Section 4(a) below.
p. "**Record Retention Schedules**" means the Company-approved schedules that set forth the relevant periods of time that particular Official Records of the Company are to be retained in the ordinary course of business to meet ATS's legal and business requirements. There are currently two (2) Record Retention Schedules: (i) for the title and escrow business (the "Title/Escrow Schedule"), (ii) for general corporate information of ATS (the "General Company Schedule").
q. "**Trade Secrets**" means information that gives ATS a competitive advantage in its markets, including information about how ATS does business, ATS's corporate, competitive, and strategic plans, pricing information, ATS's customer lists, ATS's proprietary operating data and anything else about ATS that is not public.
r. "**Training Materials**" means materials designed to train Employees about the importance of Records and how to comply with the Policy.
s. "**You**" and "**your**" means (i) an Employee with respect to that Employee's work as an employee or (ii) a 3rd Party Vendor.

2. Record Retention - Basic Procedures.

This Policy sets retention standards for Records so that (i) complete and accurate copies of Records can be located when needed; (ii) Records are stored only under authorized conditions in authorized facilities; and (iii) Records will be appropriately retired when their retention requirements have expired or their useful life has ended, unless subject to a Legal Hold Order.

To achieve the goals of this Policy,

i. Official Records will be stored, arranged and/or indexed so that they can easily and accurately be identified when required.
ii. All Records will be maintained on ATS owned or leased premises, on ATS systems, or under a contract approved by ATS's Company Legal Department with an approved 3rd Party Vendor. They should not be stored anywhere else.
iii. All Records that contain Company Information will be handled, stored and retired in such a way to maintain the confidentiality of the Company Information so that people who are not authorized to see the Company Information do not have access to it.

a. Official Records:

i. If ATS creates and uses a Record Retention Website, it will contain a list of approved locations in which Official Records should be stored. These approved locations may be electronic servers for imaged Records, local operation offices or warehouses for paper Records or other types of authorized repositories. Official Records for the applicable local offices should be stored only in those authorized locations, once identified in connection with the RRP.

ii. The Record Retention Officer will be aware of the location of where Records (Official Records and Convenience Records) are stored that are his or her responsibility. The Record Retention Officer may find it helpful to keep a master list that includes the storage locations for Records of the branch offices that are his or her responsibility.

iii. Official Records must always be kept for the specific period of time listed in the appropriate Record Retention Schedule. This is critical and is required to meet legal or business needs.

iv. Where there is only one copy of a Record, that copy is the Official Record.

v. If a Record was created in paper form but is later imaged, the image is always the Official Record. The paper document can be discarded once the document has been imaged, so long as no Legal Hold Order applies to them.

vi. If a Record exists in more than one form or if there are multiple copies of a Record, the duplicates shall be retired, so long as no Legal Hold Order applies to them.

vii. If there is any uncertainty about which constitutes the Official Record, you or your manager should consult the Record Retention Officer.

b. For Convenience Records:

i. Convenience Records will be retired as soon as we no longer need them for any business purpose, unless they are subject to a Legal Hold Order.

ii. Convenience Records that may be subject to a Legal Hold Order will be preserved in accordance with the instructions in the Legal Hold Order or as otherwise given by the Legal Hold Officer.

c. For Official Records & Convenience Records if they may be subject to a Legal Hold Order:

i. The Legal Hold Officer will issue a Legal Hold Order whenever Records may be required for a pending, or reasonably anticipated litigation, government investigation, subpoena or claim.

ii. Generally, the Legal Hold Order will cover a specific subject by name and date and will tell what categories of Records we need to keep until the Legal Hold Order is cancelled. Every Legal Hold Order will have its own Legal Hold Order ID Number.

iii. Once we receive a Legal Hold Order, we will protect and preserve any Records covered in the Legal Hold Order, even if their normal retention time has expired and even if they are Convenience Records.

iv. If you ever have any question about what Records the Legal Hold Order covers, please contact the person identified in the applicable Legal Hold Order or, if he or she is not available or if you are unsure whether any Legal Hold Order applies, contact the Legal Hold Officer. If the Legal Hold Officer is not available and your question is urgent, please contact the Record Retention Officer.

v. The Legal Hold Officer will provide you with updates on the Legal Hold Order as the matter proceeds. When requested, you should confirm to the Legal Hold Officer that you are in compliance with the Legal Hold Order.

vi. When there is no longer a need for the Legal Hold Order, the Legal Hold Officer will inform Employees and Listed Vendors subject to the Legal Hold Order that it has now been lifted.

vii. Once a Record is no longer subject to a Legal Hold Order as a result of a direction from the Legal Hold Officer, you should retain the Record for the time period set forth in the appropriate Record Retention Schedule if the Record is an Official Record (or retire it if it is a Convenience Record that has outlived its usefulness) unless the Record is subject to another Legal Hold Order.

3. Retiring Records – Basic Procedures.

a. We are expected to make sure that Convenience Records under your control are retired at the end of their useful life. We will assess periodically whether Convenience Records under your control need to be retained. Whenever a file is closed, you should review and retire any Convenience Records in that file.

b. We will not retire any Record (Official Records or Convenience Records) if any Legal Hold Order applies to that Record.

c. Whenever we retire either Official Records or Convenience Records, we will use methods appropriate to preserve the confidentiality of information in those Records. Official Records or Convenience Records containing Company Information will be retired properly and securely: (i) Company Information containing ATS's Trade Secrets, non-public personal information of past, present or potential customers or Employees (such as social security numbers, health information, credit card information and the like) will be destroyed so that it cannot be read or reconstructed and (ii) all other Company Information will be destroyed in accordance with the Company's practices applicable to such information. If you have questions, ask the Record Retention Officer regarding this.

d. Computer and IT equipment disposal carries risks to the Company after that equipment leaves the Company's premises, both environmentally (such as landfill "superfund" laws) and with respect to the potential disclosure of Company Information. ATS will contract with disposition services and uses various forensic tools to cleanse electronic data storage devices (including computers, hard drives, copiers and other equipment). If you have concerns about whether the IT Department is using the appropriate disposition services, you should raise the concerns with your Record Retention Officer.

4. Record Retention Personnel.

a. The main oversight and approval body for this Policy and the rest of the Program is the Record Retention Committee. This committee will be the final and ultimate authority for implementation and revision of this Policy and the Program.

b. The Company Record Retention Officer is a member of the Record Retention Committee. The Company Record Retention Officer is the main point of contact with Record Retention Officer and the second point of contact for Employees for routine record retention matters, including the application of the Policy.

c. A Record Retention Officer is appointed based on geographical area and is trained to serve as the administrator and first point of contact for record retention issues in a specified area. The Record Retention Officer may have other job titles as well, but when it comes to record retention, they report to the Company Record Retention Officer.

d. The Legal Hold Team will administer and implement each Legal Hold Order. The members of the Legal Hold Team may be different for different Legal Holds.

e. The Legal Hold Officer is responsible for helping to determine when a Legal Hold Order is needed, for issuing, updating, monitoring and releasing the Legal Hold Order, for answering questions about the scope and status of a Legal Hold Order and for maintaining a list of Legal Hold Orders in effect at ATS.

5. Your Record Retention Responsibilities as an Employee or Listed Vendor.

a. We will create, maintain and dispose of all Records in accordance with this Policy and the appropriate Record Retention Schedule.
b. We will properly handle Records and always respect, maintain, and enforce existing ATS safeguards against unauthorized or improper destruction of Records.
c. We will not retain Convenience Records that are copies of Official Records for longer than the underlying Official Record unless the Convenience Record is subject to a Legal Hold Order.
d. We will retain Official Records under your control for the time periods in the applicable Record Retention Schedule. If there is a business need to retain Official Records longer than the retention period in the applicable Record Retention Schedule, you must request an extension from the Local Record Retention Officer. If the Local Record Retention Officer grants the request, the applicable Official Record should be kept only for so long as designated by the Record Retention Officer and the Record Retention Officer should maintain documentation of the request and the grant until the applicable Official Record is destroyed.
e. If you receive a Legal Hold Order, you must immediately turn to it and follow all instructions in the Legal Hold Order to preserve all relevant Official Records and Convenience Records. (See Section 2(c)).
f. We will maintain the confidentiality of Records that contain Company information.
g. We will retire Records in accordance with this Policy. (See Section 3).
h. If we learn of any potential litigation, government investigation, subpoena or claim (other than the litigation of insurance claims or policies issued by ATS or to tax disputes) against ATS, you should contact the Legal Hold Officer immediately.
i. If an employee transfers to another office or department or if he/she leaves ATS's employment, he/she must notify the manager before your departure or transfer and help with the transfer of Records under his/her control.
j. Whenever an Employee transfers or leaves, managers will consult the Local Record Retention Officer and must make sure they promptly review with the Employee the status of all Records under the Employee's control.
k. If the transferring or leaving Employee has any Records that must be retained under the appropriate Record Retention Schedule or that are subject to a Legal Hold Order, the manager will take appropriate steps to ensure that the Employee's Official Records are retained for the applicable retention period and that any Official Records and/or Convenience Records of the transferred or terminated Employee are retained until the applicable Legal Hold Order(s) have been lifted.

6. Awareness of this Policy.

a. Senior management at ATS Company is responsible for distributing this Policy to ATS's Employees and 3rd Party Vendors.
b. All current Employees will receive a copy of this Policy when it is adopted.
c. All future Employees will receive the Policy when they are hired.
d. ATS will also post the current version of this Policy, along with the Record Retention Schedules, on ATS's Record Retention Website, when/if created or will post the information in the Company Employee Handbook.

e. Any ATS Employee responsible for dealing with a 3rd Party Vendor that has control of Records must provide the 3rd Party Vendor with a copy of this Policy.
f. Every 3rd Party Vendor must distribute the Policy to those of its employees who control ATS's Records, as applicable.

7. Periodic Audits.

ATS's Internal Audit Department may conduct periodic, unannounced audits of each of ATS Company's Branch locations for compliance with this Policy.

8. How to Report Violations.

a. If you suspect or know of a violation of this Policy, you should immediately notify the Record Retention Officer, and if he or she is not available, the Company Record Retention Officer or ATS's Chief Compliance Officer.
b. Your report will be kept confidential.

9. Employee Violations.

a. Because of the extreme importance of this Policy, any Employee who violates any of its terms may be subject to disciplinary actions, including but not limited to oral or written warnings, suspension or immediate termination.
b. The type of disciplinary action taken will depend on the type of violation of this Policy. ATS does not promise, imply or represent that one form of disciplinary action will occur before another.

10. Collective Effort Required to Make this Policy Work.

ATS counts on each of its Employees to make this Record Retention Policy work. If you have any suggestions on how to make it more effective or efficient, please contact ATS's Record Retention Officer.

ACTION TITLE SERVICES
of St. Johns County, Inc.

Our Email Security Policy

Action Title Services of St. Johns County, Inc. (ATS) is establishing its Email Security Policy ("ESP").

This Policy is so important that every ATS Employee at every level must learn and observe its requirements. Compliance with the ESP is an important part of every Employee's daily responsibilities and is mandatory for every Employee with respect to that Employee's work as an employee of the ATS Company and its 3rd Party Vendors.

When receiving emails:

1. We do not open emails from unknown sources.
2. We type the website address into our web browsers instead of clicking links within emails.
3. We do not click on any links or provide information to suspicious emails.

Last revision October 30, 2015 -cmh