

TIDEWATCH'S PRIVACY POLICY

TideWatch Partners, LLC ("TideWatch") is the owner and administrator of tidewatch.com. TideWatch is committed to protecting user's privacy and security. TideWatch has created this policy disclosing its information gathering and dissemination practices in order to demonstrate its firm commitment to privacy. This Privacy Policy only applies to information collected on the website located at tidewatch.com (the "Site"). Please read this notice carefully to understand TideWatch's practices. By visiting TideWatch's website, you accept the practices described in this privacy policy notice.

Information TideWatch May Collect

When you access the Site, TideWatch receives and may record information from our servers and from your browser, including your IP address, the time, assorted technical information, and information about the page you requested. These items do not disclose your name or personal identity, and are considered anonymous information.

We do not at present intend to use your personal information. However, in the future if we use your personal information in a manner different from that stated at the time of collection, we will revise this Privacy Policy and you will have a choice as to whether or not we use your information in such different manner.

Privacy Practices of Third Parties

TideWatch's website may feature links to third-party sites that offer goods, services, or information. TideWatch is not responsible for the content, privacy policies or practices of any advertisers or linked sites of any third parties. TideWatch encourages you to review the privacy policies of third parties before providing any third party with any information. Third party sites may collect and use information about you in a way that is different from this policy.

Changes to The Privacy Policy

Any change to this policy will be reflected in a new policy. TideWatch reserves the right, at its sole discretion, to amend or otherwise change the terms of this policy, at any time with or without notice. If required by law, TideWatch will post the new policy on its website and/or send you a notice of the change, in the method(s) required by applicable laws. Your continued use of TideWatch's services or any service following such notification will constitute evidence of your agreement to the revised policy.

Questions

If you have any questions about this policy notice, please call (603) 559-9999, email twp@tidewatch.com, or write to TideWatch at the following address: TideWatch, Attn: Director of Information Privacy, PO Box 219, Greenland, NH 03840.

MARKET RESEARCH PRIVACY POLICY

TideWatch Partners, llc ("TideWatch") is a market research firm that is committed to maintaining the privacy and security of personal information. TideWatch adheres to the mandated Market Research Association ("MRA") code of Standards and Ethics for Survey Research. This code includes requirements for protection of personal information and respondent identifiable information. A copy of this code can be found at <http://www.mra-net.org/>

All participant responses will be kept strictly confidential and only reported in the aggregate—that is, information about groups and not individuals—unless otherwise evident within the survey. If we indicate that personal information may be included in the research findings, we ensure that the information is treated with the strictest of confidence. We will not mislead a participant regarding the nature of the research or how the information will be used. For more information, please see the following section below entitled, "Disclosure of Personal Information".

Personal information will not be sold or traded to any other individual or company without the prior consent of the individual providing the information. We do not conduct sales or direct marketing, nor do we provide personal information to be used for direct contact sales or marketing purposes. For additional information on our company, please visit our website at www.tidewatch.com.

Disclosure of Personal Information

TideWatch limits the personal identifiable information shared with clients to that which is essential to the research project. Unless necessary for pre-research project assignments or validation, last names, phone numbers and addresses are not shared with clients or any other third party.

Personal information may be disclosed only when the survey instrument clearly states that the information will be disclosed, or when a participant makes a request during the survey that can only be fulfilled by disclosing information from the survey.

TideWatch reserves the right to disclose personally identifiable information as may be required by law or court order; notice may not be required.

In the event of a sale, merger, liquidation, dissolution, reorganization or acquisition of TideWatch, any acquiring party will be required to comply with all of the material terms of this Privacy Policy before we transfer any information to such company.

Email Addresses and Other Communication

TideWatch may have personal email addresses and phone numbers in our email system and data files that are acquired through:

- Request for information submitted to our website
- Email/phone numbers sent to TideWatch
- Research surveys completed for TideWatch
- Clients who have provided email addresses/phone numbers for research purposes

Since TideWatch does not send emails for the purpose of sales or direct marketing, the CANSPAM Act of 2003 does not apply to our email communications. However, TideWatch voluntarily observes the CAN-SPAM Act when applicable to market research. TideWatch uses email as a means of communicating to known clients and research participants.

TideWatch adheres to the following guidelines when contacting potential participants via email for an invitation to participate in opinion and marketing research.

- TideWatch will clearly identify ourselves as the sender of the email
- TideWatch will provide the appropriate contact information should the recipient of the email need to contact us with any questions or concerns
- TideWatch will provide the option to be removed from receiving additional email invitations for participation in research projects
- TideWatch will reuse email addresses only as legitimate follow up to survey research

COPPA

We are committed to protecting your child's privacy online and our practices are in full compliance with the Children's Online Privacy Protection Act (COPPA), as regulated by the FTC. This means that TideWatch does not conduct research with minors under the age of 13 without a statement of permission from the parents or guardians. To learn more about COPPA, please visit <http://www.ftc.gov/ogc/coppa1.htm>.

Questions and Concerns

For additional concerns or questions regarding our privacy policy, we may be contacted at twp@tidewatch.com or by telephone at (603) 559-9999.

Legal Disclaimer

TideWatch may disclose personal information when required by law or in the good-faith belief that such action is necessary to conform to the edicts of the law or to comply with a legal process.

Policy Changes & Updates

TideWatch reserves the right to modify this Privacy Policy at any time as we take advantage of developing technologies. Therefore, we encourage you to refer to this Privacy Policy on an ongoing basis. If we make material changes to this policy we will post notice of such changes at www.tidewatch.com.

WRITTEN INFORMATION SECURITY AND SAFEGUARDS PROGRAM

TideWatch Partners, LLC (the "Company") has developed the following Written Information Security and Safeguards Program ("Program"). Effective immediately, every employee and independent contractor is subject to the Program. Each employee and independent contractor hired by the Company after October 1, 2011 will receive a copy of the Program as part of the orientation process.

For purposes of this Program, "personal information" means: a person's first name and last name or first initial and last name in combination with any one or more of the following that relate to such person: (a) Social Security number; (b) driver's license number or state issued identification card number; (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a person's financial account; (d) medical information; (e) health insurance information; or (f) address, telephone number, or zip code; provided, however, that personal information shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public. For purposes of this Program, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional, and "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

This Program is state-neutral and intends to apply to all personal information the Company receives, maintains, processes, or otherwise has access to in connection with the provision of goods or services or in connection with employment.

I. PROGRAM OBJECTIVES

- A. To create effective administrative, technical and physical safeguards for the protection of personal information.
- B. To outline procedures for evaluating our electronic and physical methods of accessing, collecting, storing, using, transmitting and protecting personal information.
- C. To ensure the security and confidentiality of personal information.
- D. To protect against any anticipated threats or hazards to the security and/or integrity of personal information.
- E. To protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

II. DATA SECURITY COORDINATOR

The designated Data Security Coordinator (“Coordinator”) for the Company is Kristine Campel, Controller. The Coordinator maintains responsibility to:

- Implement the Program
- Conduct risk assessments of the Program as necessary
- Design and conduct training as necessary for those persons who have access to personal information to meet the goals of the Program
- Evaluate the Company’s third-party service providers ability to implement and maintain security measures for the personal information that the Company has provided access and to facilitate contracts with such third-party service providers to implement and maintain such appropriate security measures for personal information
- Coordinate with Information Technology professionals to implement the technical aspects of the Program
- Review the scope of the security measures contained herein at least annually or when there is a material change in business practices
- Conducting an annual training session for all owners, managers, employees and independent contractors, including temporary and contract employees who have access to personal information on the elements of the Program. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with Company’s requirements for ensuring the protection of personal information.
- Ensure that the appropriate oversight or audit procedures are in place to detect the improper disclosure or theft of personal information

III. RISK ASSESSMENT

The Coordinator conducts risk assessments as necessary to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of personal information that could result in its unauthorized disclosure, misuse, alteration, destruction, or other compromise, and assess the sufficiency of any safeguards in place to control these risks.

The risk assessments evaluate all relevant areas of the Company’s operations, as determined by the Coordinator. At a minimum, the risk assessment reviews:

- Employee training and management;
- Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
- Detecting, preventing and responding to cyber attacks, intrusions or other systems failures.

Once the Coordinator identifies reasonably foreseeable risks to personal information of the Company, the Coordinator will determine whether the Company’s current policies and procedures in these areas sufficiently mitigate the potential risks identified. If not, the Coordinator will amend the policies and procedures to meet the objectives of the Program.

IV. PERIODIC REEVALUATION

The Coordinator may reevaluate and modify the Program from time to time as the Coordinator deems appropriate. The Coordinator will base such reevaluation and modification on the following:

- The results of the Program's testing and monitoring efforts;
- Any material changes to the Company's operations, business or information technology arrangement; or
- Any other circumstance that the Coordinator knows has a material impact on the Program.

In order to assist the Coordinator in this regard, employees will keep the Coordinator apprised of the nature and extent of all third-party relationships and any operational changes or other matters that may impact the security or integrity of the Company's personal information.

V. EMPLOYEE TRAINING AND MANAGEMENT

In keeping with the objectives of the Program, the Company will implement, maintain and enforce the following employee management and training safeguards:

1. All employees and independent contractors are responsible for complying with this Program.
2. All new employees and independent contractors who perform services for the Company and have access to personal information will participate in the Company's information security training. Each person shall acknowledge his or her agreement to abide by the Company's Program. The training program will include, at a minimum, basic steps to maintain the security, confidentiality and integrity of personal information, such as:
 - Identifying for employees and independent contractors the types of personal information subject to protection under this Program
 - Reviewing and discussing this Program
 - Appropriately securing the physical location of personal information, including locking rooms or file cabinets, as appropriate, and safekeeping of keys and codes
 - Using password-activated computer software, systems, applications or terminals or an automatic log-off function that terminates access after a short period of inactivity
 - Using appropriate passwords
 - Changing passwords periodically, and maintaining the security of passwords
 - Transmitting personal information electronically with appropriate security
 - Appropriately disposing of paper and electronic records
 - Other training as determined appropriate by management from time to time
3. The Company takes appropriate steps to encourage awareness of and compliance with the Program.
4. All employees and independent contractors are permitted access to personal information on a "need-to-know" basis as determined by the Company.

5. Personnel shall not access, use or reproduce personal information, whether electronic or non-electronic, for their own use or for any use not authorized by the Company.
6. All persons who fail to comply with this Program shall be subject to disciplinary measures, up to and including termination of employment for employees or contract termination for independent contractors that perform services in the Company.

VI. INFORMATION SYSTEMS SAFEGUARDS

In keeping with the objectives of the Program, the Company will implement, maintain and enforce the following information systems safeguards and consult with Information Technology professionals as needed:

A. Paper Records

1. Paper or electronic records containing personal information will be stored and maintained in secure areas. The Coordinator will control access to such areas. Employees who possess keys or lock codes to such records are required to maintain such keys and codes in a secure manner as directed by the Coordinator or Department Manager.
2. Paper records containing personal information will not be left unattended at any time in an unsecured area.
3. Inactive paper records containing personal information must be placed in locked and secured container to be shredded or disposed of in another appropriate manner once the need for it is no longer required.
4. All paper records containing personal information will be properly destroyed when the Company no longer has a need to retain the personal information.

B. Electronic Records

1. The Coordinator, in conjunction with Information Technology professionals, ensures that the Company uses and maintains an appropriate level of technology for the protection of personal information.
2. The Coordinator, in conjunction with Information Technology professionals, ensures that the appropriate communication occurs with the Company's computer vendors from time to time to ensure the Company has installed the most recent patches that resolve potential software vulnerabilities.
3. The Coordinator, in conjunction with Information Technology professionals, ensures that the Company establishes procedures to preserve the security, confidentiality and integrity of personal information in the event of a computer or other technological failure.

4. Electronic personal information shall be stored on secure Company network servers.
5. The Company encourages inbound transmissions of personal information delivered to the Company via other sources be encrypted or otherwise secured.
6. All outbound transmissions of personal information must occur with an appropriate level of security and be secured in a manner acceptable to the Coordinator.
7. All hard drives, diskettes, magnetic tapes, or any other electronic media containing personal information will be erased and/or destroyed prior to disposing of computers or other hardware and as frequently as necessary as determined by the Coordinator.
8. The Coordinator conducts rolling inventory of Company computers, including any laptops and handheld devices or PDAs, on or through which personal information may be stored, accessed or transmitted to ensure these devices contain the necessary technology to secure transmissions involving personal information.
9. The Company uses anti-virus software that updates regularly.
10. The Company has installed and maintains a firewall configuration to protect accountholder data.
11. The Company controls access to electronic personal information with user identification to access its computer network.
12. The Company controls access to electronic personal information by assigning to individuals with authority to access personal information unique identifications plus passwords that are reasonably designed to maintain the security of those access controls.
13. The Company does not use vendor-supplied defaults for system passwords and other security parameters.
14. Employees and independent contractors must: (a) use passwords to the Company's computer and electronic systems only in an authorized manner; (b) respect any password-protected areas on the Company's computers and electronic systems; (c) maintain the passwords in a confidential and secure manner; and, (d) change their password on a routine basis. Employees may not, however, use password protection measures to prevent authorized representatives of the Company (e.g., the Coordinator or Information Technology personnel) from accessing any part of the Company's computer or electronic systems.
15. The Company blocks access to electronic records after multiple unsuccessful attempts to gain access.

16. Employees and independent contractors are trained in the proper use of the computer security system and the importance of personal information security.
17. The Company immediately restricts access to personal information by an employee or vendor upon their disassociation with the Company and requires the immediate return of any records containing personal information, in any form, that may at the time of such termination be in the former employee's or vendor's possession.

VII. DATA BREACH NOTIFICATION

A. Breach

The Coordinator will notify individuals if a "breach of security" of personal information occurs. A "breach of security" is the unauthorized acquisition or unauthorized use of: (1) unencrypted personal information, or encrypted electronic personal information and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, which creates a substantial risk of identity theft or fraud against that individual. A good faith but unauthorized acquisition of personal information by an employee or agent of the Company, for the lawful purposes of that employee or agent, is not a breach of security, unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

The Coordinator will also notify the owner or licensee if a "breach of security" of personal information that is not owned by the Company occurs.

Each person subject to this Program must notify the Coordinator immediately if they know, or have reason to suspect a breach of security has occurred.

B. Notification

The Coordinator shall coordinate notification to the individuals that are the subject of a data breach consistent with the applicable federal or state law or regulation where that individual resides. The notification shall at a minimum include: (1) a description of the nature and circumstances of the security breach or unauthorized acquisition or use of personal information; (2) the steps already taken or planned to be taken relative to the incident; and (3) information regarding whether law enforcement officials are engaged in investigating the incident.

C. Post-Incident Briefing

In the event of a data security breach, the Coordinator coordinates an assessment of the breach, including those individuals involved in the breach. The assessment includes discussion of the nature of the breach, corrective action taken, and amendment to the Program, if necessary, to improve security.

VIII. THIRD PARTY SERVICE PROVIDERS

The Coordinator has identified third-party service providers that have access to personal information connected with the Company. The Company has required each third-party service provider to furnish the Company with their Information Security Policy/Procedures to ensure adequate protection of personal information consistent with this Program.

Any contract entered into with a third-party service provider after March 1, 2010 will include a provision requiring the third-party service provider to implement and maintain appropriate security measures to protect personal information the Company exchanges with third-party service providers.

CLIENT LOGIN PRIVACY POLICY

For our privacy statement that governs information collected in our “Client Login” section, please click here:

https://www.tidewatch.com/clientlogin/images/stories/clientlogin_privacy.pdf