Privacy Policy

Privacy Policy

Revised: July 11, 2019

Introduction

The following is the SecurTest, Inc. and its U.S.-based subsidiary iReviewNow LLC (collectively "SecurTest" "we", "our", "us") online privacy policy, which governs how visitor information (your information) is gathered and used on SecurTest and iReviewNow Internet sites, including our EU Privacy Shield Dispute Resolution Program. Please take a few minutes to read this policy carefully.

With the limited exception of our activities under the EU-US and Swiss-US Privacy Shield Framework (see below,) SecurTest provides services to U.S. government entities, businesses, and consumers.

About SecurTest, Inc.

SecurTest, Inc. is a U.S.-based Consumer Reporting Agency (CRA) that prepares Consumer and Background Reports for authorized, users, employers and consumers under the provisions of the federal Fair Credit Reporting Act (FCRA), among other state and federal laws, rules, and regulations.

About iReviewNow, LLC

iReviewNow, LLC is a U.S.-based information company that allows consumers to securely review their consumer or background reports, dispute inaccuracies, explain adverse or derogatory information, and/or explain self-rehabilitation or improvement steps taken since the adverse actions.

Overview of our Privacy Policy

Our Privacy policy is very simple: SecurTest only collects applicant data pursuant to written Authorization and Disclosure under the FCRA and only disseminates consumer reports to employers or consumers as directed in the written authorization. In other words, data is only collected and distributed at the direction and authorization of consumers. The data is

maintained in a secured site. SecurTest maintains strict policies and procedures in all aspects of its operation to protect the privacy of consumers.

Your Information that We May Collect Online

You can affirmatively submit to SecurTest or iReviewNow certain user information pertaining to your interaction with us. User information may include a search query (such as the name and location of a business or consumer) or other information as described more fully below. You can also provide location information (so that you can search near you or in an area you specify), or billing information. We also may infer your geographic location based on your IP address or other information. User information may also include information pertaining to a complaint, such as your name, postal and e-mail address, phone and facsimile numbers, vehicle information such as vehicle identification number, and description of the complaint or customer review.

SecurTest is a provider of information and consumer reporting agency that helps businesses, non-profit organizations, and federal, state, and local governments make informed hiring and retention decisions. We screen applicants, employees and consumers, reduce fraud, mitigate risk, facilitate business decisions, and make our world safer, while protecting consumer privacy. These Privacy Principles will also help the consumer, applicant, or subject of our background screening programs understand how we use and safeguard their information, such as social security numbers and dates of birth.

Our Privacy Principles apply to Personally Identifiable Information, which includes Sensitive Personally Identifiable Information that is collected, maintained, used, or disseminated by SecurTest in delivering information products and services through any SecurTest company or line of business. Many of our products are already subject to important privacy protections provided by federal and state laws, such as the Fair Credit Reporting Act and its state law counterparts. We give careful attention to our privacy policies, which we review and change as necessary and appropriate. To underscore our commitment to privacy and our vision that good privacy is good business, we have adopted the following Privacy Principles. [1]

The policy includes our corporate privacy principles and Fair Information Practice Principles of notice, choice, access, security, and accountability. This online privacy policy applies to all sites owned and operated by:

SecurTest, Inc.
600 Grand Panama Boulevard
Suite 202
Panama City Beach, FL 32407

(800) 445-8001 - **corporatecompliance@securtest.com**

Our Websites are:

www.securtest.com
www.ireviewnow.com

Protecting Children

Our websites are not designed with the purpose of attracting any person under age 18. SecurTest does not knowingly collect or maintain any personal information from children under the age of 18, unless they have applied for employment or are employed by an employer requiring a background report, also known as a consumer report as defined by the FCRA.

Cookies and Other Persistent Identifiers

SecurTest or third parties we contract with may use persistent identifiers such as cookies, embedded scripts, web beacons, pixel tags, log files, or similar technologies to collect certain information about visitors to our site and interactions with our online and mobile information or advertisements.

For example, we may automatically collect certain non-personal information from you, including but not limited to your browser type, device type, geographical location, operating system, unique device identifier of any of your computer(s) or device(s) that are used to access the site, software version, Internet Protocol ("IP") address, phone model, phone operating system, and the domain name from which you accessed the site. We also may collect information about your use of the site, including the date and time you visit the site, the areas or pages of the site that you visit, the amount of time you spend viewing or using the site, the number of times you return to the site, other click-stream or site usage data, emails that you open, forward or click-through to our site, advertising that you click on, and other sites that you may visit.

You can still use our websites if you have set your browser to reject cookies or tracking identifiers, but it may prevent you from viewing or accessing some of the features of our sites.

Uses of Persistent Identifiers

We may use identifiers to generate certain kinds of site usage data, such as the number of hits and visits to our sites. This information is used to understand how visitors use our sites and provide better services to you. We may also use identifiers to personalize the display of services or advertisements and customize the content you see while using our sites.

We may transfer, or allow third parties to collect, analytic information about your visit to our websites to help us improve our websites and better serve you when you visit us online in the future. Analytic information may include such identifiers as your browser type, IP address, referring site URL, web pages you view and links you click on while navigating within our sites. We do not transmit Personal Identifier Information (PII), such as dates of births and social security numbers, to third parties for analytic information about your visit to our websites.

We use this information for a number of purposes, such as to provide easier site navigation, access to forms, or to track analytics and certain statistical information that enables us to improve our site and provide you with more relevant content and information on our site and other sites.

We may also use third party analytics and advertising tools, or allow third party companies, to serve ads and/or automatically collect certain non-personal information from you when you interact with our site, advertising, or social media. This may include click stream information, browser type, time and date, subject of advertisements clicked or scrolled over. These third-party tools or companies may use technology such as cookies, web beacons, pixel tags, or log files to collect such information.

How We Use Your Information

We will use information you affirmatively submit to us for the purpose for which it is submitted, such as to reply to your email, respond to your inquiry, handle your background request, publish your customer review or comment, process billing transactions, register your participation for one or more of our services or products, respond to requests related to program participation, review applications for employment, and communicate with you when necessary. We may also use such information to provide operational notices, in program record-keeping and to conduct research on industry marketplace practices. We may publish aggregate data, but the aggregate data will not include any user information you provided to us.

We may use third party contractors to act on our behalf, and these contractors are obligated to not disclose or use your information for other purposes.

We rely on information collected from our users to develop new services and conduct analysis to enhance current content and services. Information collected from you may be used to review usage and operations of our site and address any resulting issues with our site.

At certain points where your information is collected on our site, there may be a box where you may indicate you would like to be on a mailing list to receive information about our services or products. This election box only appears in places where the service collecting your information maintains such lists. You can remove your name from our mailing list by utilizing the appropriate unsubscribe feature contained in the emails.

We may also use the information we collect from you to enhance your online experience and provide you with customized site content and targeted information on the site, across third party sites, or through your mobile device.

Other Purposes

We may also share your information under the following circumstances:

We respond to requests from governmental agencies or where required by law (such as by subpoena, investigative demand, court order or regulation).

We may share information where our records indicate a company may be engaged in fraudulent activity or other unfair or deceptive practices that we believe should be referred to a governmental agency or a private organization whose work is consistent with our mission;

We may share information with appropriate governmental authorities, where warranted by a

company's failure to comply with various federal or state laws or regulations.

We may share information with appropriate persons or governmental authorities, where your communication suggests possible harm to others.

International Transfers

If you are visiting our site from outside the United States, be aware that your information will be transferred to, and maintained on, computers located within the United States. The collection, use, retention and any other processing of your information will be governed by United States law and further by the specific jurisdictions within the United States where that information is stored, unless otherwise specified. Please refer to the Privacy Shield section below for more information regarding data transferred from the EU or Switzerland to the United States pursuant to the Privacy Shield Frameworks.

LEGAL COMPLIANCE

SecurTest requires clients to adhere to all laws, including all federal and state laws, the Equal Employment Opportunity Commission (EEOC) and their state and local counterparts, and the Fair Credit Report Act, among any others that apply.

The Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of personal information maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual. (SecurTest is not a federal agency as defined by the Privacy Act of 1974. However, our guiding principles use applicable or similar privacy rules that are listed in the Act, such as “No Disclosure without Your Consent” and our methods for safeguarding your information.)

INFORMATION COLLECTION - Personally-Identifiable Information

These sites only collect Personally Identifiable Information (“PII”) from you based on your authorization, such as for a background investigation with an employer, prospective employer, government entity, or contractor of a government entity. PII collected with your consent may include, for example, name, e-mail address, resume information, address, telephone number, date of birth, social security number, driver’s license or government identification numbers, or any inquiries you may make directly through our websites or that you have authorized a SecurTest client to provide for a background report.

How We Protect Personally Identifiable Information

1. You must consent to provide PII information about yourself.

2. We collect PII information securely via secure online (internet), fax, mail, or other secure systems that only our clients, the consumer, and SecurTest can view.

3. We do not sell or redistribute your PII information to third parties. Except where required by

our federal government clients, our background reports do not contain any PII information. Thus, the report does not include your date of birth or social security number. Where a federal government user, such as the Department of Defense (DoD) and its military branches, requires PII information in our background reports, the report can only be viewed through secure online access that meets the strict security procedures approved by the DoD.

4. We need your social security number, date of birth, address, name, maiden name, and other names to perform the background investigation. We also need your driver's license number if we are required to report your driving record. We use this information to check court and other government records to ensure that we find and only report information about you. An accurate background investigation cannot be performed without PII information, since a name match could result in reporting inaccurate information or information that is not your background or record.

Credit Reports

Some employers or authorized users require a credit report as part of their application or employment requirements. We follow U.S. federal and state laws, including the Fair Credit Reporting Act (FCRA) and California laws, among others.

We strongly encourage consumers/applicants to check their credit reports free athttp://www.annualcreditreport.com. Three credit bureaus collect and report credit information. Checking your credit before applying for employment or before authorizing a credit report allows you to identify any inaccurate information with these credit bureaus. SecurTest does not collect credit information and only reports the credit bureau report where you have authorized the report. SecurTest has no method to correct credit bureau reports, and as such, the consumer assumes all responsibilities for contacting credit bureaus if the credit file or report contains any inaccuracies.

INFORMATION USE AND CONSUMER CHOICE

The information collected by our websites is used only for responding to your inquiries or those authorized by you and our clients. We may contact you in response to your comments or inquiries, as part of the maintenance of your account with us (if you have one), or in order to complete a background investigation or compliance process, which will assist in ensuring the accuracy of our reports and compliance with the Fair Credit Reporting Act, among other state and federal laws. If you decide that you do not want to receive further e-mails from SecurTest, you can reply to the e-mail and place in the subject line, "OPT OUT." You may also call 800-445-8001 with a request that we not continue to e-mail you. We do not use outside data sources to enrich marketing data obtained online. We do not use any information about you, including email addresses, except in compliance with our duties and obligations.

ACCESS AND CORRECTION

As an information company, we value having our data as accurate as possible. Accordingly, we strive to maintain the accuracy of the information collected through our websites. As the inventor of iReviewNow, we have the only consumer-friendly transparent system for you to

ensure background and consumer reports are accurate and accessible to you at the same time as the employer or entity you authorized for us to prepare a report. You are our most important tool in ensuring that their data is complete and accurate. We will provide you access to your personally identifiable information for as long as we maintain that information in an accessible format. Similarly, we permit and encourage you to correct inaccuracies in the information you submit to us through our websites, by email, telephone, or using iReviewNow. If you wish to correct any inaccurate information you have submitted to any of these sites, please call (800) 445-8001. SECURITY We take steps to protect against the loss, misuse, or unauthorized alteration of personally identifiable information collected through this website. We recognize the importance of security for all personally identifiable information collected by our website. We exercise care in providing secure transmission of your information. Once we receive personally identifiable information, we take steps to protect its security on our systems. In the event we request or transmit sensitive information, such as Social Security Numbers, we use accepted industry standards, such encryption programs and software. We strictly limit access to personally identifiable information to those employees who need access in order to carry out their job responsibilities. All of our employees have undergone extensive background screening, FASTscreen testing, and have their criminal history reviewed every 90 days to ensure your information is in trusted hands.

POLICY CHANGES

We reserve the right the revise this policy as needed. As such, in the event revisions are made, we will prominently post announcements on our websites that describe the details of the revisions.

PERSONAL INFORMATION DISCLOSURE: UNITED STATES OR OVERSEAS

In preparing a consumer report or investigative consumer report, we only send information about the subject of the report outside the United States if our client or you ask for information from a jurisdiction outside the United States. For example, if a prospective employee worked outside of the United States, our client might ask for a criminal history report for the country in which the prospective employee worked. When we do this kind of report, we send enough information to identify the subject of the report. We do not send your personal identifier information outside the United States except where such is required to conduct a background investigation, which is authorized by the subject of the investigation.

OPT-OUT OPTION

You Can Opt Out of Receiving Further Marketing from SecurTest at any time. We will send you information about our various products and services or other products and services we feel may be of interest to you. If you do not want to receive such mailings, simply tell us when you give us your personal information. Alternatively, at any time you can easily opt out of receiving further marketing from SecurTest by emailing us at optout@securtest.com. Please type "OPT OUT" in the subject line of your email.

CALIFORNIA PRIVACY RIGHTS

California Civil Code Section 1798.83 permits customers or subjects of our background reports (consumer reports) of SecurTest, Inc. who are California residents to request certain information regarding its disclosure of personal information to third parties for their direct marketing purposes. To make such a request, please send an e-mail to CaliforniaRequest@securtest.com or write us: SecurTest, Inc. California Consumer Protection Department 600 Grand Panama Boulevard, Suite 202, Panama City Beach, FL 32407

Use of Credit Reports – California Residents

SecurTest generally does not provide credit reports where the subject of the report lives in California due to Assembly Bill 22 that became effective on January 1, 2012. California clients requesting credit reports MUST ensure compliance with all applicable laws and provide proof of the need for a credit report as part of the consumer authorization. Employers must adhere to the California law, as there are strict rules and restrictions on ordering and using consumer credit reports for hiring or employment purposes. Clients with applicants or employees residing in California that require credit reports as part of the employment process are required to submit a separate authorization and statement of purpose that the subject of the investigation must sign when ordering such credit reports from SecurTest.

FREQUENTLY ASKED QUESTIONS

How secure is my information? SecurTest recognizes the importance of secure online transactions and takes steps to safeguard the privacy of information you provide through online forms. For your online authorization or use of iReviewNow, programs encrypt the information you provide on the request form before transmission to our secure computer systems. This information is decrypted only upon receipt by us. Physical, electronic, and procedural safeguards designed to guard your personally identifiable information are maintained in strict adherence to government and industry regulations and standards. Further, our website's security protocols and measures are designed to protect the personally identifiable information you provide from unauthorized access or alteration. These measures include physical security, technological security measures, and encryption of certain information.

Is it safe to provide my Social Security Number, government issued identification number or Date of Birth? You must provide your Social Security Number, Date of Birth, and at times government issued identification numbers, such as passport or driver's license numbers for us to conduct a background investigation. We use this information to ensure we only report records associated with you, as a name match could result in reporting information that is not your record. The site's security protocols and measures are designed to protect the personally identifiable information you provide from unauthorized access or alteration. As an added security measure, except when your report is transmitted to those entities requiring your PII data, such as government users, we do not report your date of birth and mask your social security number where no more than the last four digits are visible.

How does the online authentication process work? To assure that we have your consent to conduct the background investigation, we require that you have signed an authorization form

or given authorization by electronic signature. An electronic signature is a specific process wherein you consent to the background check, our policies, and our procedures as if signing the document. The End-User of our reports have agreed to securely store your authorizations. Often your authorizations are securely transmitted to SecurTest or iReviewNow and securely stored on our computer servers or systems. We authenticate your identity utilizing the personal identification information you provide, including, but not limited to, your Social Security number and date of birth. For your protection, if your identity cannot be authenticated, you will receive further instructions on how to verify your identity. Failure to authenticate your identity is not an indicator of fraudulent activity or identity theft.

How can I learn more about guarding against internet fraud and protecting my personal information? OnGuardOnline.gov provides practical tips from the federal government and the technology industry to help you be on guard against phishing and internet fraud, secure your computer, and protect your personal information.

How do I request a "fraud alert" be placed on credit file? You have the right to ask that nationwide consumer credit reporting companies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide consumer credit reporting companies. As soon as that agency processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file.

- **Equifax: 1-877-576-5734. www.alerts.equifax.com**
- **Experian: 1-888-397-3742. www.experian.com/fraud**
- **TransUnion: 1-800-680-7289. www.transunion.com**

DATA INTEGRITY AND SECURITY

SecurTest and iReviewNow uses reasonable efforts to maintain the accuracy and integrity of Personal Data and to update it as appropriate. We have implemented physical and technical safeguards to protect Personal Data from loss, misuse, and unauthorized access, disclosure, alternation, or destruction. For example, electronically stored Personal Data is stored on a secure network with firewall protection, and access to SecurTest's electronic information systems requires user authentication via password or similar means. SecurTest also employs access restrictions, limiting the scope of Employees who have access to Data Subjects' Personal Data.

Further, SecurTest uses secure encryption technology to protect certain categories of data. All data is encrypted (for example using HTTPS) when it is transmitted outside SecurTest's firewall, and certain types of data are encrypted at all times in the System. Despite these precautions, no data security safeguards guarantee 100% security all of the time.

Jurisdiction

You agree in using our websites that jurisdiction shall be in Bay County, Florida, USA where

allowed by law.

Updates

If we change this policy in the future, we will post the changes here and indicate the date of the changes at the top of the policy.

Problems or Complaints with Our Privacy Policy

If you have a complaint about our compliance with this privacy policy, you may contact us at privacy@securtest.com.

Privacy Shield Frameworks for Data Transferred to the United States from the EU/Switzerland

SecurTest complies with the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries (including Iceland, Liechtenstein, and Norway) and Switzerland transferred to the United States pursuant to Privacy Shield. SecurTest has certified that it adheres to the Privacy Shield Principles with respect to such data. If there is any conflict between the policies in this privacy policy and data subject rights under the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit https://www.privacyshield.gov/

With respect to personal data received or transferred pursuant to the Privacy Shield Frameworks, SecurTest is subject to the regulatory and enforcement powers of the U.S. Federal Trade Commission.

Pursuant to the Privacy Shield Frameworks, EU and Swiss individuals have the right to obtain our confirmation of whether we maintain personal information relating to you in the United States. Upon request, we will provide you with access to the personal information that we hold about you. You may also may correct, amend, or delete the personal information we hold about you. An individual who seeks access, or who seeks to correct, amend, or delete inaccurate data transferred to the United States under Privacy Shield, should direct their query to privacyshield@securtest.com. If requested to remove data, we will respond within a reasonable timeframe.

We will also provide an individual opt-out choice, or opt-in for sensitive data, before we share your data with third parties other than our agents, or before we use it for a purpose other than which it was originally collected or subsequently authorized. To request to limit the use and disclosure of your personal information, please submit a written request to privacyshield@securtest.com.

In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

SecurTest's accountability for personal data that it receives in the United States under the Privacy Shield and subsequently transfers to a third party is described in the Privacy Shield Principles. In particular, SecurTest remains responsible and liable under the Privacy Shield Principles if third-party agents that it engages to process the personal data on its behalf do so in a manner inconsistent with the Principles, unless SecurTest proves that it is not responsible for the event giving rise to the damage.

In compliance with the Privacy Shield Principles, SecurTest commits to resolve complaints about your privacy and our collection or use of your personal information transferred to the United States pursuant to Privacy Shield. European Union and Swiss individuals with Privacy Shield inquiries or complaints should first contact SecurTest at privacyshield@securtest.com by contacting Steven C. Millwee, CPP, the president and CEO.

SecurTest has further committed to refer unresolved privacy complaints under the Privacy Shield Principles to an independent dispute resolution mechanism, the BBB EU PRIVACY SHIELD. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit http://www.bbb.org/EU-privacy-shield/for-eu-consumers for more information and to file a complaint. This service is provided free of charge to you.

If your complaint involves human resources data transferred to the United States from the EU and/or Switzerland in the context of the employment relationship, and SecurTest does not address it satisfactorily, SecurTest commits to cooperate with the panel established by the EU data protection authorities (DPA Panel) and/or the Swiss Federal Data Protection and Information Commissioner, as applicable, and to comply with the advice given by the DPA panel and/or Commissioner, as applicable, with regard to such human resources data. To pursue an unresolved human resources complaint, you should contact the state or national data protection or labor authority in the appropriate jurisdiction. Complaints related to human resources data should not be addressed to the BBB EU PRIVACY SHIELD.

Contact details for the EU data protection authorities can be found at http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm.

If your Privacy Shield complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See Privacy Shield Annex 1 at https://www.privacyshield.gov/article?id=ANNEX-I-introduction.

iReviewNow – the New Protection Standard

Our founder, Steven C. Millwee, is the inventor of the proprietary patented iReviewNow System (U.S. Patents 7,979,908, 8,646,101 and 9,183,363) that helps applicants, employees, and consumers better protect themselves from inaccurate information and identity theft or fraud. At the same time, iReviewNow provides employers, prospective employers, or other authorized organizations a better picture of an individual's background and qualifications. When a background investigation report contains adverse information that might impact a

hiring, retention, employment, credit granting, insurance issuance, or other legal decision, iReviewNow becomes part of the report at the option of the client or consumer. Unless we are contracted to do so, our clients give the subject a copy of the adverse report and our iReviewNow in real-time to ensure compliance with the FCRA and other laws and rules. The subject immediately authenticates or disputes information and provides additional insight that will help the user of the report make informed decisions, while mitigating claims of inaccuracy, discrimination, and other types of misuse or abuse of the report.

Organizations using iReviewNow expand their pool of qualified applicants as they get real-time usable information authenticated by the subject. This helps mitigate risks and claims from consumers, applicants, and employees who otherwise must wait to receive a notice by mail of adverse information or decisions. Consumers, subjects of our background investigations and reports, and users of the reports can opt-in or opt-out of using iReviewNow. Using iReviewNow ensures the consumer sees his or her report at the same time as the prospective employer or user of the report.

Our patented iReviewNow allows consumers, applicants, employees and/or subjects of background reports to receive a copy of the report through secure online access, email, or mail when the subject does not have internet access. Our background screening solutions are the most transparent system, integrating the subject into the process.

How to Contact Us

If you need further assistance regarding the above rights, please contact us using the contact information provided below and we will consider your request in accordance with applicable law.

SecurTest, Inc.
600 Grand Panama Boulevard
Suite 202
Panama City Beach, FL 32407

(800) 445-8001 - corporatecompliance@securtest.com

Our Websites are:

www.securtest.com
www.ireviewnow.com

PDF Version: http://www.securtest.com/privacypolicy.pdf

Footnote References:

1 Individually identifiable Information from or about an individual consumer including, but not limited to: (a) a first and last name or first initial and last name; (b) a home or other physical address, which includes at least the street name and name of city or town; (c) an email address; (d) a telephone number; (e) a Social Security number; (f) credit and/or debit card information, including credit and/or debit card number with expiration date; (g) date of birth;

(h) a driver's license number; or (i) any other information from or about an individual consumer that is combined with (a) through (h) above. Download PDF Copy of these policies at http://www.securtest.com/SecurTestprivacy.pdf