

Privacy Policy

Privacy Statement

Seccuri, Inc.

Last Modified: June 5, 2024

1. Introduction

Seccuri, Inc., with mailing address of 701 Brickell Key Blvd, Miami FL 33131 and Juanita Isabel Duque (CEO and co-founder) as the data controller (“Seccuri, Inc.,” “we,” or “us”), explains in this Privacy Policy (the “Policy”) how we collect, process and/or use information that we receive via our website, emails we send, and mobile applications, including <https://www.seccuri.com>, (the “Site”) that link to this Policy, as amended from time to time.

At Seccuri, Inc., our purpose is to our mission is to help close the 4M+ cybersecurity talent shortage that exists worldwide by using our specialized AI algorithm to help grow and improve the cybersecurity workforce through smart matching of company jobs and top Talent, career orientation tools for both cybersecurity enthusiasts and professionals, and a training ecosystem to upskill and reskill.

Respecting your personal data is crucial to our mission, which is why we make sure your information is well protected and handled properly.

As the Global Cybersecurity Skills and Talent Platform, Seccuri, Inc. fulfills distinct roles. Either when we are acting as intermediaries between Companies and Talent users who are looking to initiate a recruitment process, as well as when we are offering Companies and Talent users training opportunities from our Training Ecosystem partners or evaluating Talent user profiles to provide career path suggestions, we only collect and use personal information as authorized by our Company clients and Talent users to help connect top Talent user candidates to Company clients’ job opportunities, and help Talent users grow in their professional cybersecurity careers through career advancement resources and tools such as our Training Ecosystem and Career Path orientation module. If you by any means have any questions about how your information is being handled by our Company clients or Training Ecosystem partners, or desire to exercise your rights, please contact them directly.

This Policy describes how Seccuri, Inc. collects, processes, uses, shares, and protects the Personal Data you provide. It also describes your choices regarding use, access, and correction of your Personal Data.

Our registered users share their professional identities, engage with their network, exchange knowledge and professional insights, learn and develop skills, and find business and career opportunities. Content and data on some of our services is viewable to non-members, which include training and certification companies of which Seccuri has partnerships with.

We use the term “Designated Countries” to refer to countries in the European Union (EU), European Economic Area (EEA), and Switzerland.

This Policy applies to information we collect:

-
- On our Site: in email, text, and other electronic messages between you and our team.
 - It does not apply to information collected by us offline or through any other means, including on any other website operated by us or any third-party; or
 - Any third party, including through any application or content (including advertising) that may link to or be accessible from or on the Site.

Please read this Policy carefully to understand our policies and practices regarding your information and how we will treat it. If you do not agree with our policies and practices, your choice is not to use our Sites. By accessing or using our Sites, you agree to this Policy. This Policy may change from time to time (see Updates to Our Privacy Policy). Your continued use of the Sites after we make changes is deemed to be acceptance of those changes, so please check this Privacy periodically for updates.

This Privacy Policy applies to seccuri.com and other Seccuri-related sites, apps, communications, and services, but excluding services that state that they are offered under a different privacy policy. For California residents, additional disclosures required by California law may be found in our California Privacy Disclosure.

Changes to Our Privacy Policy

Changes to the Privacy Policy apply to your use of our Services after the “effective date.”

Seccuri, Inc. (“we” or “us”) can modify this Privacy Policy, and if we make material changes to it, we will provide notice through our Services, or by other means, to provide you the opportunity to review the changes before they become effective. If you object to any changes, you may close your account.

You acknowledge that your continued use of our Services after we publish or send a notice about our changes to this Privacy Policy means that the collection, use and sharing of your personal data is subject to the updated Privacy Policy, as of its effective date.

2. Definitions

- **Account:** means a unique account created for You to access our Service or parts of our Service.
- **Company:** (referred to as either "the Company", "We", "Us" or "Our" in this Agreement) refers to Seccuri, Inc. For the purpose of the GDPR, the Company is the Data Controller.
- **Consent of the Data Subject:** means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- **Cookies:** are small files that are placed on Your computer, mobile device, or any other device by a website, containing the details of Your browsing history on that website among its many uses.
- **Company Account:** is a type of Seccuri platform user specifically designated to all its Company clients. It includes Company users seeking to find Top Cybersecurity Talent, Talent candidates for job postings, or to train and manage their current workforces' skillsets.
- **Cyber Team:** A registered Company user or Company client can track its current employees' cybersecurity career development by inviting them to register at Seccuri AI as Talent users. Once signed up, they will be able to connect to your Company's profile and become part of your Seccuri's Cyber Team.
- **Data Controller:** for the purposes of the GDPR (General Data Protection Regulation), refers to the Company as the legal person which alone or jointly with others determines the purposes and means of the processing of Personal Data.
- **Device:** means any device that can access the Service such as a computer, a cell phone, or a digital tablet.

- **Enterprise:** means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity.
- **Personal Data Breach:** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
- **Personal Data:** is any information that relates to an identified or identifiable individual. For the purposes of GDPR, Personal Data means any information relating to You such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity.
- **Processing:** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- **Site / Service:** refers to the Seccuri Website and Seccuri Platform.
- **Talent User / Talent Account:** is a type of Seccuri user designated for cybersecurity professionals, enthusiasts or people interested in cybersecurity, and accessing to all our Talent Services within the Seccuri Platform.
- **Third Party:** means a natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorized to process personal data.
- **Usage Data:** refers to data collected automatically, either generated by the use of the Service or from the Service infrastructure itself (for example, the duration of a page visit).
- **Website:** refers to Seccuri, accessible from [WEBSITE_URL]
- **You:** means the individual accessing or using the Service, or the company, or other legal entity on behalf of which such individual is accessing or using the Service, as applicable. Under GDPR (General Data Protection Regulation), You can be referred to as the Data Subject or as the User as you are the individual using the Service.

2. Summary

Our Privacy Policy explains the following:

A. Information We Collect About You and How We Collect It

We collect diverse types of information about you, including information that may directly identify you, information that is about you but individually does not personally identify you, and information that we combine with our other users. This

includes information that we collect, information you give us, and information we collect automatically.

Privacy Information may include, but is not limited to:

- Email address
- First name and Last name
- Phone number
- Billing address, State, Province, ZIP/Postal code, City
- Professional profile
- Education
- Work experience
- Technical Skills associated to cybersecurity
- Score in MBTI test
- Photo
- Usage data

Other personal Information collected by us may include general usage metrics of the Platform, your financial payment information, your profile, email communication history with Seccuri, Inc., anything you submit to or post on the Site, and other information associated with you or your organization, as well as other information that may or may not specifically identify you.

The legal name and definition of personal information differs from jurisdiction to jurisdiction. Seccuri, Inc. will not use or share Personal Information other than as described in this Privacy Policy.

Usage Data

Usage Data is collected automatically when using our Service, or through any other digital or personal communication between you and us.

Usage Data may include information such as Your Device's Internet Protocol address (e.g., IP address), browser type, browser version, the pages of our Service that You visit, the time and date of Your visit, the time spent on those pages, unique device identifiers and other diagnostic data. When You access the Service by or through a mobile device, We may collect certain information automatically, including, but not limited to, the type of mobile device You use, Your mobile device unique ID, the IP address of Your mobile device, Your mobile operating system, the type of mobile Internet browser You use, unique device identifiers and other diagnostic data. We may also collect information that Your browser sends whenever You visit our Service or when You access the Service by or through a mobile device.

The information collected through the Platform may be stored on servers, clouds (such as Microsoft Azure, Amazon AWS, among others), computers, or other media located in the countries where our Enterprise currently holds its operations and processes data. These countries currently include United States, Spain, and Colombia. We may also collect general information about your technology interfaces or preferences and the websites you visit. We may use a third-party provider to process financial and payment information.

The information that is stored is kept in encrypted databases with strict policies for remote network and administrative user access. These databases are hosted in Microsoft Azure clouds and respective data centers, ensuring compliance with the provider's security policies.

You do not have to provide additional information on your profile; however, profile information helps you to get more from our Services, including helping business opportunities find you. It is your choice whether to include sensitive information on your profile and to make that sensitive information public. Please do not post or add personal data to your profile that you would not want to be publicly available.

We collect personal data from you when you provide, post or upload it to our Services, such as when you fill out a form, (e.g., with demographic data or salary), respond to a survey, or submit a resume or fill out a job application on our Services.

You do not have to post or upload personal data; though if you do not, it may limit your ability to grow and engage with your network over our Services.

We also may collect public information about you, such as professional-related news and accomplishments, and make it available as part of our Services, as permitted by your settings.

We may obtain information about you from third-party sources, such as Google or Apple. This information may be utilized, analyzed, and/or compared with information that Seccuri, Inc. has collected from you or that you have submitted to the Platform. If Seccuri, Inc. obtains information from third-party sources, you agree that your sole legal remedy for any harm associated with that information is against the third-party that provided the information to us, and that you will not

assert any cause of action, claim or demand against us other than requesting we delete any erroneous information.

For the avoidance of doubt, Seccuri, Inc. shall be entitled to collect anonymous and/or aggregated data across its various products and services provided that no individual natural person can be identified from such data (“Aggregate Data”). The Aggregate Data will be used for various purposes, including without limitation to analyze behavior, trends, and website interaction, and to improve, and enhance our services and for other development, creation of new features, diagnostic and corrective purposes in connection with our services. Seccuri, Inc. shall own all right, title, and interest in and to the Aggregate Data and this is not considered personal data.

If you are in the “Designated Countries,” Seccuri, Inc. will be the controller of your personal data provided to, or collected by or for, or processed in connection with our Services.

If you are outside of the Designated Countries, Seccuri, Inc. will be the controller of your personal data provided to, or collected by or for, or processed in connection with, our Services.

As a visitor or non-registered user of Seccuri, the collection, use and sharing of your personal data is subject to this Privacy Policy and other documents referenced in this Privacy Policy, as well as updates.

Information Collection Technology

For each visitor to our Site, we may use various technologies, including “Cookies” to automatically gather certain information pursuant to your use of the Site, from your electronic device about your activities using the Site. We may collect and store non-personally identifying information through cookies, and third parties to

profile user activity and preferences. Technical and specification information about your device and settings may be collected when you use the Site. This information includes internet protocol (IP) addresses, browser type, internet service provider (ISP), referring/exit pages, operating system, date/time stamp, the content of previously accepted “cookies” from us, and clickstream data. We collect and store this information on an individual basis and in combined forms. We also collect both user-specific and aggregate information on what pages visitors access or visit.

A Cookie is data stored on your device that tracks non-personal information about you. We use cookies on our Site to help you navigate efficiently and perform certain functions. Moreover, we may assign your device one or more cookies that enable us to improve the quality of the Sites and to personalize your experience. Cookies allow us to automatically collect information about your activity on the Websites, such as the content you access while using the Site, the links you click, and other activity you conduct while using the Site.

We also use third-party cookies that help us analyze how you use this website, store your preferences, and provide the content and advertisements that are relevant to you. These cookies will only be stored in your browser with your prior consent.

You may choose to modify your device setting to disable cookies or limit their use. If you choose to disable or limit cookies, or otherwise limit your device permissions to the Site, you may experience diminished performance from the Site and/or may be prevented from using some or all features of the Site.

You will find detailed information about all cookies under each consent category below. The cookies that are categorized as "Necessary" are stored on your browser as they are essential for enabling the basic functionalities of the site.

Our cookies generally fall into two categories: Necessary and Uncategorized.

- **Essential cookies:** Necessary cookies are required to enable the basic features of this site, such as providing secure log-in or adjusting your consent preferences. These cookies do not store any personally identifiable data.

Cookie	ARRAffinity
Duration	Session
Description	ARRAffinity cookie is set by Azure app service and allows the service to choose the right instance established by a user to deliver subsequent requests made by that user.

Cookie	ARRAffinitySameSite
Duration	Session
Description	This cookie is set by Windows Azure cloud and is used for load balancing to make sure the visitor page requests are routed to the same server in any browsing session.

Administered by: Us

- **Uncategorized cookies:** Other uncategorized cookies are those that are being analyzed and have not been classified into a category as yet.

Administered by: Us

You can change your cookie preferences or withdraw your consent right away at any time through the cookie consent banner displayed on the Site.

Our Platform may contain web beacons (also known as “clear gifs”) or similar technologies that gather non-personally identifiable information about your use of our Platform. Such technology may also be contained in e-mail messages or newsletters from us that allow us to determine whether messages have been accessed. The purpose of our use of this technology is so that we may analyze the effectiveness of our marketing efforts and the quality of our Platform.

We log usage data when You visit or otherwise use our Services, including our platform technology, such as when you view or click on content (e.g., job posting) or ads (on or off our sites), perform a search, share articles, or apply for jobs. We use logins, cookies, device information and internet protocol (“IP”) addresses to identify you and log your use.

One of our main sources of data collection comes from our Seccuri Platform, where both Talent and Company users need to register to be able to access all our service portfolio. After the registration process, both users are then invited to log in to their account and complete their user profile in the Edit Profile section. The information that ends up being collected by our Seccuri Platform (if provided by the Company or Talent user) will then be stored in our databases hosted on Microsoft Azure cloud and used only for the purposes described in this Policy.

We also collect information about you when you send, receive, or engage with messages in connection with our Services. For example, if you send a message to a Company when interested in applying to one of their job postings, we track whether you have acted on it and will send you reminders.

Other

Our Services are dynamic, and we often introduce new features, which may require the collection of new information. If we collect materially different personal data or materially change how we collect, use, or share your data, we will notify you and may also modify this Privacy Policy.

B. How We Use Information

We use your Personal Data for various purposes described below, including to:

- **Provide our Site to You and maintain our Service**, including monitoring its usage.
- **To manage Your Account**: to manage Your registration as a user of the Service. The Personal Data You provide can give You access to different functionalities of the Service that are available to You as a registered user.
- **To contact You**: To contact You by email, telephone calls, SMS, or other equivalent forms of electronic communication, such as a mobile application's push notifications regarding updates or informative communications related to the functionalities, products, or contracted services, including the security updates, when necessary or reasonable for their implementation.
- **To provide you with information you request from us.**
- **Verify your identity**: for example, when you return to the Site and have already logged in.
- **Enforce our rights arising from contracts.**
- **For the performance of a contract**: the development, compliance and undertaking of the purchase contract for the products, items, or services You have purchased or of any other contract with Us through the Service.
- **To manage Your requests**: To attend and manage Your requests to Us.
- **To provide You** with news, special offers and general information about other services and events (from Seccuri, Inc. and third parties that Seccuri, Inc. selects).
- which we offer that are similar to those that you have already purchased or enquired about unless You have opted not to receive such information.
- **Notify you about changes.**

- **Provide you with notices about your account.**
- **For other purposes:** We may use Your information for other purposes, such as data analysis, identifying usage trends, determining the effectiveness of our promotional campaigns and to evaluate and improve our Service, products, services, marketing, and your experience.

We use the data that we have about you to provide and personalize our Services, including with the help of automated systems and inferences we make, so that our Services can be more relevant and useful to you and others.

It is your choice whether to invite someone to our Services or send a message request. When you invite someone to review your profile, your invitation will include your network and basic profile information (e.g., name, profile photo, job title, region). We will send invitation reminders to the person you invited.

We may share Your personal information in the following situations:

-
- **With Service Providers:** We may share Your personal information with Service Providers to enhance, develop, monitor, and/or analyze the use of our Service, for payment processing, to contact You.
 - **With Company Users:** We may share or transfer Your personal information to Company users and clients who are looking to contact you as a potential job candidate (just in case you have previously given us your personal consent to do so) or in case your Talent account currently holds a validated relation with one of our Company clients.
 - **With Business Partners:** We may share Your information with Our business partners, including those from our Training Ecosystem, in which case we will require those Partners to honor this Privacy Policy. Business Partners include for example our Training Providers, which offer You certain products, services, or promotions.
 - **With other users:** when You share personal information or otherwise interact in the public areas with other users, such information may be viewed by all users and may be publicly distributed outside.
 - **With Your consent:** We may disclose Your personal information for any other purpose with Your consent.
-

Stay Informed

Our Services allow you to stay informed about news, events, and ideas regarding professional topics you care about, and from professionals you respect. Our Services also allow you to improve your professional skills or learn new ones. We use the data we have about you (e.g., data you provide, data we collect from your engagement with our Services and inferences we make from the data we have about you), to personalize our Services for you, such as by recommending or ranking relevant content and conversations on our Services.

We also use the data we have about you to suggest skills you could add to your profile and skills that you might need to pursue your next opportunity. So, if you let us know that you are interested in a new skill, we will use this information to personalize content in your feed, suggest that you take certain courses or trainings promoted in our site, or suggest related learning content to help you towards that new skill. We use your content, activity, and other data, including your name and photo, to provide notices to your network and others.

Career Advancement

Our Services allow you to explore career paths, evaluate educational opportunities, and seek out, and be found for, career opportunities. Your profile can be found by those looking to hire (for a job or a specific task) or be hired by you. We will use your data to recommend jobs, show you and others relevant professional contacts (e.g., who work at a company, in an industry, function or location or have certain skills and connections). You can signal that you are interested in changing jobs and share information with Companies. We will use your data to recommend jobs to you and you to Company users seeking to hire Talent users. We may use automated systems to provide content and recommendations to help make our Services more relevant to our users, Visitors, and customers. Keeping your profile accurate and up to date may help you better connect to others and to opportunities through our Services.

Productivity

Our Services allow you to search for potential employees or employers to do business with. Our Services allow you to communicate with other Members and schedule and prepare meetings with them. If your settings allow, we scan

messages to provide “bots” or similar tools that facilitate tasks such as scheduling meetings, drafting responses, summarizing messages, or recommending next steps.

Communications

We will contact you through email, mobile phone, notices posted on our, and other ways through our Services, including text messages and push notifications. We will send you messages about the availability of our Services, security, or other service-related issues. We also send messages about how to use our Services, network updates, reminders, job suggestions and promotional messages from us and our partners. You may change your communication preferences at any time. Please be aware that you cannot opt out of receiving service messages from us, including security and legal notices.

Marketing

In addition to advertising our Services, we use Members’ data and content for invitations and communications promoting membership and network growth, engagement, and our Services, such as by showing your connections that you have used a feature on our Services.

Customer Support

We use data (which can include your communications) to investigate, respond to and resolve complaints and for Service issues (e.g., bugs).

Insights That Do Not Identify You

We use your data to produce and share insights that do not identify you. For example, we may use your data to generate statistics about our members, their profession or industry, to calculate ad impressions served or clicked on, or to publish visitor demographics for a Service or create demographic workforce insights.

Security and Investigations

We use your data (including your communications) for security purposes or to prevent or investigate possible fraud or other violations and/or attempts to harm our users, visitors, or others.

Lawful Basis for Processing Your Personal Data

We have a lawful basis for our processing of your Personal Data, including processing for our legitimate interests (when balanced against your rights and freedoms), to fulfill our obligations to you under a contract with you, and required by law, and with your consent.

C. How We Protect Personal Data

At Seccuri, safeguarding user data is our top priority. We employ robust security measures to ensure the confidentiality, integrity, and availability of this information. We protect user data through:

- **Encrypted Databases:** All stored information resides in encrypted databases. These databases are accessible only to authorized personnel, and strict access controls are enforced.
- **Microsoft Azure Cloud and Data Centers:** Our databases are hosted in Microsoft Azure cloud and data centers. Azure adheres to industry-leading security standards, ensuring compliance with security policies.
- **Change Logs:** We maintain detailed logs to track any modifications to candidate data. This allows us to validate changes and maintain data integrity.
- **Personal Data Retention:** We keep your personal data as long as your account is open or necessary for providing our services. This includes data provided by you or others, as well as usage data generated from your

interactions. We may retain certain information in depersonalized or aggregated form.

- **Legal Obligations and Usage Data:** We also retain your data to comply with legal requirements, resolve disputes, and enforce agreements. Usage data is generally retained for shorter periods, but security enhancements or legal obligations may extend retention periods.
- **Data Subject Rights:** Users have the right to access, rectify, and delete their information.
- **Opt-In Marketing Emails:** We obtain explicit consent from candidates before sending marketing emails. Candidates have the option to receive or opt out of such communications.
- **Incident Monitoring:** Through Azure, we continuously monitor our databases for security incidents. Any anomalies trigger immediate investigation and remediation.
- **Risk Mitigation:** We proactively address risks related to configuration and modification. Regular security assessments help us identify and mitigate potential vulnerabilities.
- **Performance Metrics:** We monitor performance indicators and capacity metrics for our Azure services. This ensures optimal performance while maintaining security.
- **Cookies and tracking:** We use cookies to enhance your experience on our website. Cookies help with efficient navigation, improve performance, and personalize content. Third-party cookies analyze user behavior. You can modify your device settings to manage cookies.
- **Employee Training:** Our staff undergoes regular security awareness training to enhance awareness and adherence to security best practices.
- **Privacy by design:** Functional and technical platform designs have privacy built in as core commandments.

D. Permissions

Children Under the Age of thirteen (13)

In accordance with COPPA (Children's Online Privacy Protection Act), our Site is not intended for children under the age of 13 and children under the age of 13 are not permitted to use our Site. We will remove any information about a child under the age of 13 if we become aware of it.

We do not knowingly collect personally identifiable information from anyone under the age of 13. If You are a parent or guardian and You are aware that Your child has provided Us with Personal Data, please contact Us.

If We need to rely on consent as a legal basis for processing Your information and Your country requires consent from a parent, We may require Your parent's consent before We collect and use that information.

E. How We Share Your Personal Data

Your information, including Personal Data, is processed, and stored exclusively by Microsoft Azure Cloud. All our data centers and cloud are hosted by Microsoft Azure following all privacy requirements that Microsoft follows to guarantee compliance in usage and processing of data.

Your submission of such information represents your consent to its processing within the Azure Cloud.

The Company takes all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy. We utilize Microsoft Azure's secure infrastructure, which includes advanced security measures such as data encryption, strict access controls, compliance with industry standards, and regular security assessments to protect your data and personal information.

We do not share, sell, or otherwise disclose your Personal Data for purposes other than those outlined in this Policy. We may use and share your information for any legally permissible purpose. We may match, use, and share any of the information we collect from you to third parties, including:

- Our future subsidiaries and our affiliates.
- Our third-party service providers that we use to support our business, including Training Ecosystem Partners who offer their programs in the Seccuri Training Ecosystem (marketplace).
- To a company we merge with, acquire, or that buys us, or in the event of a change in structure of our company of any form.
- To Company Clients or Company users looking to contact Seccuri Talent users (if the case applies and if consented to be an eligible candidate) for job opportunities.
- To Company Clients or Company users looking to contact and manage the skillsets of their Cyber Team members.
- Under certain circumstances, the Company may be required to disclose Your Personal Data if required to do so by law or in response to valid requests by public authorities (e.g., a court or a government agency).
- To comply with other legal obligations.
- To enforce our rights; and
- With your consent.

The ways we may use or share information that we collect about you include:

- Providing you with use of the Site.
- Providing you with products or services, whether from Seccuri, Inc., or any - related organizations, entities, or affiliates.
- Providing you with customized content and services.
- Providing technical or customer support.
- Performing research and analysis to gauge the use of the Site.
- Communicating with you by e-mail, telephone, text message, and/or mobile devices about products or services that may be of interest to you from Seccuri, Inc., any affiliates, sponsors or other third parties.
- Enforcing this Privacy Policy, other Seccuri, Inc. posted policies, enforce Seccuri, Inc. agreements, or otherwise manage its business.
- Performing functions as otherwise described to you at the time of collection.

To perform certain services on your behalf, we may publish certain information that you provide. You agree that any testimonial feedback, posts, interactions, or other comments provided by you to Seccuri, Inc. through any form of communication including but not limited to through the Site, becomes the sole and exclusive property of Seccuri, Inc. and that such information may be used for any legally permissible purpose, including, but not limited to marketing and advertising our Site.

You acknowledge and agree that, unless otherwise prohibited by law, Seccuri, Inc. may use and disclose your personal and non-personal information to public or private third-parties: (i) for inspection by law enforcement officials (including in the case of potential criminal activity); (ii) to respond to cease and desist letters, arbitration proceedings, legal actions and suits, criminal and civil subpoenas, any court orders; (iii) to enforce or apply the terms of this Privacy Policy or any other agreement between us; and (iv) to protect our, our users, and others' rights, property, or safety whether during or after the term of your use of our Platform.

Profile

Your profile is fully visible to You and other users of our Services (e.g., Company users interested in finding top candidates for their job postings, managing career paths from Talent users associated to their Cyber Teams, or Talent users who

make part of the Seccuri community and are looking to apply to job postings or entail communications with other Seccuri users) if you approve.

The information provided by Talent users in their profile completion may be used for candidate review by Seccuri's Company users who have posted jobs and/or are interested in contacting Talent users for their job postings or are looking to manage and track their Cyber Team's professional career paths.

Moreover, our specialized AI algorithm, which was created to help close the cybersecurity talent gap that exists worldwide, is intended to make automated decisions based on the Talent users' current cybersecurity profile (defined according to the information provided by these users in the 'Edit Profile' section) to match them quickly and smartly to Company job postings and offer them career advancement recommendations.

Subject to your settings, you may manage who can see your profile including others using our Services (e.g., Company users or users of third- party search engines).

Legal Disclosures

It is possible that we will need to disclose information about you when required by law, subpoena, or other legal process or if we have a good faith belief that disclosure is reasonably necessary to (1) investigate, prevent or take action regarding suspected or actual illegal activities or to assist government enforcement agencies; (2) enforce our agreements with you; (3) investigate and defend ourselves against any third-party claims or allegations; (4) protect the security or integrity of our Services (such as by sharing with companies facing similar threats); or (5) exercise or protect the rights and safety of Seccuri, Inc., our users, personnel or others. We attempt to notify users about legal demands for their personal data when appropriate in our judgment, unless prohibited by law or court order or when the request is an emergency. We may dispute such demands when we believe, in our discretion, that the requests are overbroad, vague or lack proper authority, but we do not promise to challenge every demand.

Change in Control or Sale

We can also share your personal data as part of a sale, merger or change in control, or in preparation for any of these events. Any other entity which buys us, or part of our business, will have the right to continue to use your data, but only in the manner set out in this Privacy Policy unless you agree otherwise.

F. Protection of User Information

We maintain administrative, physical, and technical safeguards for all user information collected on our Site. However, given the nature of communications and information technology, and that the use of the Internet has inherent risks, although we regularly monitor for possible vulnerabilities and attack, we cannot warrant or guarantee that information provided to us through the Site or stored in our systems or otherwise will be absolutely free from unauthorized intrusion by others, nor can we warrant or guarantee that such data may not be accessed, disclosed, altered, or destroyed by breach of any of our physical, technical, or managerial safeguards. Therefore, although we take reasonable steps to secure your information, we cannot and do not promise or warrant that your information will always remain secure.

External links and third-party privacy practices

Seccuri, Inc. cannot guarantee or verify the contents of any externally linked website. You should therefore note you click on external links at your own risk and Seccuri, Inc. cannot be held liable for any damages or implications caused by visiting any external links. This Privacy Policy does not cover any third party's use or handling of your information once it is shared. Instead, the privacy policy of the third-party will govern. We encourage you to visit the websites of those third parties and fully read and understand their privacy policies. Some of these entities will have different privacy terms than we do, and their servers may be located outside the United States.

The Site may link to other websites. We disclaim any and all responsibility for the privacy practices of third parties that may have links to or from our Site. We encourage you to review the privacy policies and privacy statements of every website that you visit that collects personally identifiable information.

International Resident Rights

You may have certain rights under applicable data protection laws, including the right to access and update your Personal Data, restrict how it is used, transfer certain Personal Data to another controller, withdraw your consent at any time, and the right to have us erase certain Personal Data about you. You also have the right to complain to a supervisory authority about our processing of your Personal Data.

Consent to Processing Outside the European Economic Area

We may process your Personal Data outside of your home country, including to the United States. We only do this when we are legally permitted to do so and when we have appropriate safeguards in place to protect your Personal Data.

G. Detailed Information on the Processing of Your Personal Data

The Service Providers We use may have access to Your Personal Data. These third parties, including Seccuri's Company clients and Business Partners may collect, store, use, process, and transfer information about Your activity on Our Service in accordance with their Privacy Policies.

Analytics

We may use third-party Service providers to monitor and analyze the use of our Service such as Google Analytics, Smartlook, Clicky, Matomo, among others.

Email Marketing

We may use Your Personal Data to contact You with newsletters, marketing or promotional materials and other information that may be of interest to You.

You may opt-out of receiving any, or all, of these communications from Us by following the unsubscribe link or instructions provided in any email We send or by contacting Us.

- Seccuri Scoop Newsletter (sent every 2 weeks via email)
- Weekly Blog updates (sent every week via email)
- Any other marketing communication made and sent by Us with Platform updates, news, events, etc.

Payments

We may provide paid products and/or services within the Seccuri Platform. In that case, we may use third-party services for payment processing (e.g., payment processors).

We will not store or collect Your payment card details. That information is provided directly to Our third-party payment processors whose use of Your personal information is governed by their Privacy Policy.

These payment processors adhere to the standards set by PCI-DSS as managed by the PCI Security Standards Council, which is a joint effort of brands like Visa, Mastercard, American Express and Discover. PCI-DSS requirements help ensure the secure handling of payment information. Our main payment processor is currently Stripe, Inc.

H. User's Choices and Obligations

Data Retention

We generally retain your personal data as long as you keep your account open or as needed to provide you Services. This includes data you or others provided to us and data generated or inferred from your use of our Services. Even if you only use our Services when looking for a new job every few years, we will retain your information and keep your profile open, unless you close your account. In some cases, we choose to retain certain information (e.g., insights about Services use) in a depersonalized or aggregated form.

We will also retain and use Your Personal Data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies. Moreover, We will also retain Usage Data for internal analysis purposes. Usage Data is generally retained for a shorter period of time, except when this data is used to strengthen the security or to improve the functionality of Our Service, or We are legally obligated to retain this data for longer time periods.

Rights to Access and Control Your Personal Data

We provide many choices about the collection, use and sharing of your data, from deleting or correcting data you include in your profile and controlling the visibility of your posts to advertising opt-outs and communication controls. We offer you settings to control and manage the personal data we have about you.

The rights You have in relation to your personal data include:

-
- To access the personal data held by Seccuri, Inc. about You
 - To opt out of receiving marketing communications any time
 - Where you have provided personal data voluntarily, or otherwise consented to its use, the right to withdraw Your consent.
 - The right to complain to a data protection authority.
 - The Right to Human Intervention
-

For personal data that we have about you, you can:

-
- **Delete Data:** You can ask us to erase or delete all or some of your personal data (e.g., if it is no longer necessary to provide Services to you). You can also choose to delete your Seccuri account at any given moment, along with all the information you have voluntarily provided the Seccuri Platform, by logging in to your account and following the steps provided for account deletion under the 'Settings' section. Once the account has been deleted, all the data belonging to your Seccuri account will also be immediately erased from our databases.
 - **Change or Correct Data:** You can edit your personal data at any given moment through your Seccuri account. To do so, please sign in to the Seccuri Platform and navigate through the 'Edit Profile' section where you will be able to directly correct or change your data. Once finished, please remember to save your profile for the Platform to immediately update your personal information. You can also ask us to change, update or fix your data in certain cases by emailing us at contact@seccuri.com, particularly if it is inaccurate.
 - **Object to, or Limit or Restrict, Use of Data:** You can ask us to stop using all or some of your personal data (e.g., if we have no legal right to keep using it) or to limit our use of it (e.g., if your personal data is inaccurate or unlawfully held).
 - **Right to Access and/or Take Your Data:** You can ask us for a copy of the personal data you provided in a machine-readable form. To request this copy, please email us at contact@seccuri.com. Once your request has been sent to us, our team at Seccuri will make sure to extract all your personal information from our databases, import it to a readable document such as an Excel file, and send it to you via email (all within the next 24 hours of the request reception).
-

Please be aware that, in certain circumstances, where you do not provide personal information, which is required by us, we will not be able to provide the services under our contract with You or Your Company or may not be able to comply with a legal obligation on us. For example, when acquiring a Seccuri Subscription Plan or a program from our Training Ecosystem, we will require information such as your name, and payment information. You will be made aware if this situation arises and what the consequences of not providing the personal information will be.

You may also contact us using the contact information below, and we will consider your request in accordance with applicable laws.

Closing Your Account and Data Retention Periods

We retain your Personal Data for as long as you keep your account open. To voluntarily delete your Seccuri account, you can log in to the Platform with your username and password at any moment, browse the 'Settings' module found under the 'Profile' section, and follow the instructions to delete your Talent or Company account. Once your account has been successfully deleted, all personal information provided to you from us will be automatically deleted from our database and will no longer be stored nor processed by Seccuri, Inc.

By registering at the Seccuri Platform you are giving consent that you have read and accepted our Terms and Conditions and the Privacy Policy presented to You in this document. However, you are free to withdraw at any given moment. If this is the case and you decide to opt out on the established agreements (in case You do not agree on the established terms or on any of their modifications), you can follow the steps mentioned above to delete your account.

In some instances, we may keep it after you close your account, for example we may keep it:

- On our backup and disaster recovery systems;
- For as long as necessary to protect our legal interests; and
- To comply with other legal requirements.

We retain your personal data even after you have closed your account if reasonably necessary to comply with our legal obligations (including law enforcement requests), meet regulatory requirements, resolve disputes, maintain security, prevent fraud and abuse, enforce our User Agreement, or fulfill your request to "unsubscribe" from further messages from us. We will retain de-personalized information after your account has been closed.

I. Security Safeguards

Information transmitted over the Internet is not completely secure, but we institute measures designed to protect your Personal Data. You can help protect your Personal Data and other information by keeping your password to our Sites confidential.

We implement security safeguards designed to protect your data, such as HTTPS, and regularly monitor our systems for possible vulnerabilities and attacks. However, we cannot guarantee the security of any information that you send us. There is no guarantee that data may not be accessed, disclosed, altered, or destroyed by breach of any of our physical, technical, or managerial safeguards.

Data Controller, Data Protection Officer, and Representative

Seccuri, Inc. is the Data Controller of the Personal Data you provide on the Site, as well as the Company users or Company clients who register in the Seccuri Platform with the purpose of finding and contacting registered Talent users who might be of interest to fill in a cybersecurity job position, and/or managing the cybersecurity career development of those internal employees who have also registered as Talent users in the Seccuri Platform and are part of their Cyber Team. As Data Controllers, both Seccuri, Inc. and its Company clients are responsible for protecting Talent users' data and using it lawfully.

Employers, or recruiters who serve as their company's main representatives to candidates, determine the purpose of collecting candidate personal data. This makes them the data controllers who are fully responsible for protecting candidate data and using it lawfully.

Cross-Border Data Transfers

At Seccuri, we are committed to protecting your privacy and ensuring the security of your data. All of Seccuri's data centers are hosted exclusively by Microsoft Azure, and though following all privacy, storage, and management of data follows best practices by Microsoft Azure.

To store and manage user data securely, Seccuri utilizes Microsoft Azure's cloud services. Microsoft Azure is renowned for its robust security measures and adherence to strict regulatory standards. By partnering with Microsoft Azure, we ensure that all data is stored in compliance with relevant data protection laws, including the following measures:

- **Data Encryption:** Data is encrypted both at rest and in transit using advanced encryption protocols, ensuring that unauthorized parties cannot access your information.
- **Access Controls:** We implement strict access controls and regularly audit access permissions to ensure that only authorized personnel have access to your data.

- **Compliance with Standards:** Microsoft Azure complies with various industry standards and regulations such as ISO/IEC 27001, SOC 1, SOC 2, and SOC 3. These certifications affirm Azure's commitment to data security and privacy.
- **Regular Security Assessments:** We conduct regular security assessments and audits in collaboration with Microsoft Azure to identify and mitigate any potential vulnerabilities in our data storage practices.

By leveraging Microsoft Azure's secure infrastructure, Securi ensures that your data is protected under the highest standards of data security and privacy within the United States. We are committed to maintaining the confidentiality, integrity, and availability of your data, and we continuously work to uphold these principles in all our data handling practices.

You may request more information about the safeguard that we have put in place in respect to transfer of personal data by contacting us as the contact section below.

Incident Response Plan

At Securi, we prioritize the security and privacy of our users' data. In the event of a data breach or security incident, we follow a comprehensive Incident Response Plan to mitigate the impact and ensure transparency. Our process includes the following steps:

1. Detection and Identification:

- **Continuous Monitoring:** We use advanced security tools and monitoring systems to detect potential breaches in real-time.
- **Incident Identification:** As soon as a potential incident is detected, our security team assesses and identifies the nature and scope of the incident.

2. Containment:

- **Immediate Action:** We take immediate steps to contain the breach and prevent further unauthorized access. This includes isolating affected systems and securing data.
- **Temporary Solutions:** Implement short-term fixes to mitigate the immediate risk.

3. Eradication:

- **Root Cause Analysis:** Investigate and determine the root cause of the breach.
- **Remove Threat:** Eliminate the threat by removing malware, closing vulnerabilities, and applying necessary patches.

4. Recovery:

- Restore Systems: Safely restore and verify the integrity of affected systems and data.
- Continuous Monitoring: Monitor systems to ensure no further compromise occurs during the recovery process.

5. Notification

- User Notification: Notify affected users promptly if their data has been compromised, providing information on the breach and steps they can take to protect themselves.
- Regulatory Compliance: Inform relevant regulatory bodies as required by law and comply with all applicable breach notification requirements.

6. Post-Incident Analysis

- Incident Report: Document the incident, response actions, and outcomes in a detailed report.
- Lessons Learned: Conduct a thorough review to understand what happened and how to prevent future incidents.
- Improve Security: Update our security policies, tools, and training based on insights gained from the incident.

7. Communication

- Transparency: Maintain open communication with users, stakeholders, and regulatory bodies throughout the incident response process.
- Support: Provide ongoing support to affected users and address their concerns promptly.

Direct Marketing and Do Not Track Signals

We currently do not share personal data with third parties for their direct marketing purposes without your permission.

J. GDPR Privacy Policy

GDPR Principles

Securi, Inc. complies with the principles of GDPR. The six overall guiding principles are as follows:

- Lawfulness, transparency, and fairness
- Purpose limitation
- Data minimization
- Accuracy

- Storage limitation
- Confidentiality and integrity

Your privacy and security are of foremost importance to us. We make sure to always follow these principles and ask you how you would like us (or our partners) to communicate with you.

Legal Basis for Processing Personal Data under GDPR

We may process Your Personal Data under the following conditions:

- **Consent:** You have given Your consent for processing Personal Data for one or more specific purposes.
- **Performance of a contract and/or Platform registration:** Provision of Personal Data is necessary for the performance of an agreement with You and/or for any pre-contractual obligations thereof, or Your previous registration to our Seccuri Platform as a Company or Talent user.
- **Legal obligations:** Processing Personal Data is necessary for compliance with a legal obligation to which Seccuri, inc. is subject.
- **Vital interests:** Processing Personal Data is necessary in order to protect Your vital interests or of another natural person.
- **Public interests:** Processing Personal Data is related to a task that is carried out in the public interest or in the exercise of official authority vested in the Company.
- **Legitimate interests:** Processing Personal Data is necessary for the purposes of the legitimate interests pursued by the Company.

In any case, Seccuri, Inc. will gladly help to clarify the specific legal basis that applies to the processing.

Your Rights under the GDPR

Seccuri, Inc. undertakes to respect the confidentiality of Your Personal Data and to guarantee You can exercise Your rights.

You have the right under this Privacy Policy, and by law if You are within the EU, to:

- **Request access to Your Personal Data:** The right to access, update or delete the information We have on You. Whenever made possible, you can access, update or request deletion of Your Personal Data directly within Your account settings section by login in at <https://platform.seccuri.com/#/>. If you are unable to perform these actions yourself, please contact Us at contact@seccuri.com to assist You. This also enables You to receive a copy of the Personal Data We hold about You.

- **Request correction of the Personal Data that We hold about You:** You have the right to have any incomplete or inaccurate information We hold about You corrected. You can correct your Personal Data by editing your profile information, after having signed in to your Seccuri account at <https://platform.seccuri.com/#/>.
- **Object to processing of Your Personal Data:** This right exists where We are relying on a legitimate interest as the legal basis for Our processing and there is something about Your particular situation, which makes You want to object to our processing of Your Personal Data on this ground. You also have the right to object to where We are processing Your Personal Data for direct marketing purposes.
- **Request erasure of Your Personal Data:** You have the right to ask Us to delete or remove Personal Data when there is no good reason for Us to continue processing it. You can also erase Your Personal Data at any given moment by signing into your Seccuri account at <https://platform.seccuri.com/#/> and choosing and accepting to delete your account under the 'Settings' menu. By deleting your account, all the data and content associated with your profile will be officially erased.
- **Request the transfer of Your Personal Data:** We will provide to You, or to a third-party You have chosen, Your Personal Data in a structured, commonly used, machine-readable format. Please note that this right only applies to automated information which You initially provided consent for Us to use or where We used the information to perform a contract with You.
- **Withdraw Your consent:** You have the right to withdraw Your consent on using your Personal Data. If You withdraw Your consent, We may not be able to provide You with access to certain specific functionalities of the Seccuri Platform.

Exercising of Your GDPR Data Protection Rights

You may exercise Your rights of access, rectification, cancellation, and opposition by contacting Us via email at contact@seccuri.com. Please note that we may ask You to verify Your identity before responding to such requests. If You make a request, a Seccuri representative will try to respond to You as soon as possible.

You have the right to complain to a Data Protection Authority about Our collection and use of Your Personal Data. For more information, if You are in the European Economic Area (EEA), please contact Your local data protection authority in the EEA.

K. Updates to Our Privacy Policy

We may update Our Privacy Policy from time to time, and we will post any changes to our Policy on our Site. If we make material changes to our Policy, we may notify you of such changes through your contact information and invite you to review (and accept, if necessary) the changes.

You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.

L. Contact Us

For additional information pertaining to our Privacy Policy or desire to defend any of the rights described in this Privacy Policy, please contact us at contact@seccuri.com or by writing us at:

Seccuri, Inc.
Attn: Chief Security Officer
701 Brickell Key Blvd
Miami, Florida 33131