LEGAL AND CYBERSECURITY FAQs

1) Who is Criteria and what service do you provide?

Criteria is a leading talent success company, providing scientifically designed and validated pre- and post-hire assessments, video interviewing, and talent management tools through our web-based **software as a service (SaaS)** annual subscription. We have an active customer subscriber base of nearly 5,000 businesses, that range from government agencies and Fortune 100 companies to medium and small businesses in virtually every industry. We have customers in 60 countries with assessments provided in numerous foreign languages. These businesses use Criteria to make objective, evidence-based talent decisions that reduce bias and drive better hiring, performance, and retention outcomes for their teams.

Criteria assessments and score reports are science-based, using empirical evidence from Criteria's 15+ year history in addition to that of the recently acquired Australian company, Revelian, and its 20+ year history. We have administered over 40,000,000 assessments for more than 1,100 job positions, under the supervision of our world renown industrial/organizational (I/O) psychologists and Scientific Advisory Board, and we are constantly analyzing the over one billion data responses to continually improve the predictive validity of our tests and our score reports while reducing bias.

All Criteria customers benefit from our high-quality, cost-effective platform with continued new features, enhancements, and assessments, as well as individualized and targeted candidate assessment profiles that rely upon our enormous data lake of anonymized results gathered from all our customers. These profiles allow for comparisons to the same or similar positions and industries throughout our customer population, to everyone's benefit.

Criteria customers achieve an average of:

- 52% better hiring success
- 29% greater productivity
- 25% more revenue from sales
- 29% greater productivity
- 48% lower turnover

2) What type of personal data do you collect and where is it stored?

While we do not require highly sensitive personally identifiable information (PII) for customers and candidates, cybersecurity and legal compliance are both paramount concerns and ongoing priority initiatives at Criteria. We normally collect a candidate's name and email, making it easier for our customers who may or may not be using an applicant tracking system. There is an option to collect resumes and job applications as well, but that is customer-selectable; it is not required. We do not collect highly sensitive personally identifiable information from candidates; **Criteria does not need, and does not collect, HIPAA, financial, or other highly sensitive information.**

In the candidate assessment process, we do have one candidate-optional section that allows for anonymous collection of certain candidate demographic data. The data obtained is anonymized and aggregate demographic information is only used internally, by our industrial/organizational (I/O) psychologists, to continually refine our assessment items, identify any potential disparate impact, and reduce bias. If requested by a customer and provided the sample size is large enough to insure anonymity. We may provide some anonymized and aggregate reporting to customers who have a legitimate regulatory need for such reporting.

Depending upon where you are located, your data will be stored in one of two Amazon Web Services (AWS) locations. Generally, customers in North America, South America, and Europe will have their data stored in the United States AWS

location while customers in Australia and the Asia-Pacific region will have their data stored in the Australia AWS location.

3) Are you GDPR-compliant, CCPA and CPRA compliant, and do you abide by the Australian Privacy Principles and Mandatory Breach Notification Scheme?

Yes, Criteria is ISO 27001:2013-certified and we are compliant with:

- European Union General Data Protection Regulations
- California Consumer Privacy Act
- Australian Privacy Principles
- Australian Mandatory Breach Notification Scheme

In addition, our credit card processor, Stripe ensures that the Criteria Service is fully compliant with the Payment Card Industry Data Security Standard (PCI DSS).

4) What other cybersecurity measures do you have in place?

As previously mentioned, cybersecurity is one of our top priorities. Our stability and commitment to implementing leading-edge security practices protect your data. The Criteria data ecosystem is continuously monitored to maintain a high standard of security, availability, and performance that our customers and candidates can rely on. We have both automated security testing and we use third-party penetration testing to stay ahead of potential threats to your data.

All data at Criteria is encrypted both in transit and at rest using AES-256 encryption.

Our cloud-based platform is hosted entirely on Amazon Web Services (AWS), which boasts robust built-in privacy features and provides end-to-end security and is highly scalable. To learn more about AWS security and its features, head to https://aws.amazon.com/securityhttps://aws.amazon.com/security/. AWS has all major cybersecurity certifications including SOC 2 Type 2.

Every Criteria employee must pass a thorough cognitive aptitude and personality assessment as well as a criminal background check prior to being hired. Each employee is then trained, according to their job role, but all employees are trained on and held to rigorous cybersecurity policies and procedures to prevent data breaches and keep your information safe.

Please click this link to access our Trust Center (https://www.criteriacorp.com/security-and-compliancewhere) where you will have access to all our cybersecurity and legal documentation. Level 1 documentation is not restricted, however the more detailed Level 2 documentation will require DocuSign execution of a non-disclosure agreement.

Included in the Trust Center is Please see Criteria's Data Processing Addendum where we incorporate the European Commission's Standard Contractual Clauses for data transfer between EU and non-EU countries and to learn how we process and handle your data.

Our commitment to security extends beyond how we maintain our platform – we keep our tests just as secure. We use dynamic testing to mitigate the risk of cheating, employ adaptive testing techniques, and can flag inconsistencies in responses. Visit Criteria's Test Security page to learn more.

4) Will you complete a cybersecurity questionnaire/audit or new vendor form that we require of all our vendors?

Your sales executive can complete most simple cybersecurity and new vendor forms. If you need more detailed cybersecurity information we ask that you please reference the Cloud Security Alliance (CSA) STAR (Security, Trust,

Assurance, Risk) registry where you can review our responses to their CAIQ (Consensus Assessment Initiative Questionnaire) questions.

The CSA STAR Registry is a publicly accessible registry that documents the security and privacy controls provided by popular cloud computing offerings. STAR encompasses the key principles of transparency, rigorous auditing, and harmonization of standards outlined in the Cloud Controls Matrix (CCM). Publishing to the registry allows organizations to show current and potential customers their security and compliance posture, including the regulations, standards, and frameworks they adhere to. It ultimately reduces complexity and helps alleviate the need to fill out multiple customer questionnaires.

We will provide you with all the documentation that your cybersecurity and legal teams will need (including cybersecurity level 1 and level 2 information). For more detailed questions, we rely on the STAR registry to ensure you can quickly get the information you need. Unfortunately, with over 5,000 active customers, it simply is not scalable to complete individual, customized forms for our customers.

However, we love to communicate, so if you have specific needs or requests, let your sales executive or customer success manager know. We are happy to set up calls with our consulting I/O psychologists, our cybersecurity team, or attorneys from our Business Affairs department. We have found that an audio or video call helps answer customer questions fully and quickly.

5) What, exactly, is a SaaS provider?

Software as a service (SaaS) is a software distribution model in which a cloud provider hosts applications and makes them accessible to end users over the world wide web, the Internet. As a SaaS provider we leverage the state-of-the-art service, reliability, and industry-leading security of our Internet hosting provider, Amazon Web Services (AWS).

We have designed the Criteria platform to be extremely configurable/customizable, and test batteries allow for various test selections, but being a SaaS provider we must rely upon consistent terms, policies, and procedures that allow us to efficiently scale and continually improve our Service.

6) Can we use our contract and our own DPA, instead of Criteria's?

We understand that you prefer your own agreement, as it has been written based on your business and vetted by your attorneys. Unfortunately, your contract is not designed for our Service. We're sure you understand that being a SaaS provider with nearly 5,000 active customers, we cannot have custom agreements for each and every customer; it does not scale.

Our MSA is a simple agreement that clearly identifies the specific terms within the Service subscription.

If you are a governmental or in a highly regulated industry, please notify your Sales Executive or Customer Success Manager who can create a service ticket to arrange for a call with our attorneys or cybersecurity technicians, where we may be able to accommodate your requirement via an addendum to our MSA.

7) I have specific requirements, integration with my ATS, and specific reporting requirements.

We support API integrations (tests and video) with most Applicant Tracking Systems (ATS) and we are continually adding new integrations; however, we are not a custom development house or a work-for-hire provider. As a SaaS, we are constantly adding new features and functionality that are suggested by our Customer Advisory Committee, "crowd-sourced" by our customers, recommended by current industrial organizational (I/O) psychology research, and recommended by our People & Culture team who use our Service for all our hiring.

So, even though we do not create bespoke assessments or allow custom agreements for every customer, our high-quality cost-effective solution provides reliable, consistent results, and allows for industry-leading user-customizable features. Depending upon the contract tier, we offer consulting from our (IO) psychologists as well as individualized case studies, assessment validation studies, and custom score reports.

8) Do you have cybersecurity insurance?

Yes, Criteria carries all major insurance coverage for its global operations including cyber coverage (US10,000,000) that includes technology errors & omissions, cyber liability, breach costs, and eCrime.

9) How do I access your legal and cybersecurity information?

Below is a list of (and link to) the numerous cybersecurity and legal resources you will find on our website. If you prefer, you can ask your sales executive or customer success manager to send PDFs directly to you by email. Please note: For security purposes, our level 2 cybersecurity information requires you to sign our non-disclosure agreement Sign Non-Disclosure Agreement (NDA).

Here is a list of the various documentation we have available (if PDF format):

CYBERSECURITY DOCUMENTATION
(included in the Trust Center)

- ISO Certification (Level 1)
- List of Cybersecurity Policies (Level 1)
    - Cybersecurity Incident Plan
    - Disaster Recovery
    - Business Continuity
    - Data Retention
- Technical Details (Level 2, MNDA required)
- CAIQ Spreadsheet (Level 2, MNDA required)
- Pen Test Summary (Level 2, MNDA required)
- PCI Vulnerability Scan (Level 2, MNDA required)

LEGAL DOCUMENTATION

- Terms and Conditions of Use (TCU)
- Data Processing Addendum (DPA)
- Privacy Policy
- Acceptable Use Policy (AUP)
- Digital Millennium Copyright Act Policy (DMCA)