

Cloud SaaS Terms and Conditions (v2.10)

Last Updated: August 1, 2026

These Cloud SaaS Terms and Conditions together with all referenced exhibits, policies, order/cart pages, checkout pages, statements of work, and other documents incorporated by reference, collectively the **"Agreement,"** govern access to and use of the cloud-based software-as-a-service products, modules, bundles, applications, websites, APIs, AI-enabled features, documentation, support services, and related services made available by **GZYN Inc.,** a **California Corporation** with offices in **San Francisco, Bay Area, California** ("**Company,**" "**we,**" "**us,**" or "**our**").

By clicking "**I agree,**" creating an account, completing checkout, starting a trial, accessing or using the Services, or authorizing any person to access or use the Services, you agree to this Agreement on behalf of yourself and, if applicable, the company or other legal entity you represent. If you are accepting this Agreement on behalf of an entity, you represent and warrant that you have authority to bind that entity.

The person or entity accepting this Agreement is referred to as "**Customer,**" "**you,**" or "**your.**"

If you do not agree to this Agreement, do not access or use the Services.

1. Definitions

For purposes of this Agreement:

- 1.1. "**Account**" means Customer's account for accessing and administering the Services.
- 1.2. "**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with a party.
- 1.3. "**AI Features**" means any features, workflows, outputs, recommendations, analyses, classifications, summaries, ratings, rankings, matching, generation, extraction, or other functionality that uses artificial intelligence, machine learning, large language models, foundation models, generative AI, or similar technologies.
- 1.4. "**Cloud Providers**" means third-party providers of Cloud infrastructure, Cloud APIs, Cloud Storage or related technology used by Company to provide Product Features, which may include Google Cloud Platform, Amazon Web Services (AWS), MicroSoft Azure and other providers.
- 1.5. "**AI Providers**" means third-party providers of AI models, AI APIs, OCR APIs, infrastructure, or related technology used by Company to provide AI Features, which may include OpenAI, Google/Gemini, Anthropic, and other providers.
- 1.6. "**Authorized User**" means an individual employee, contractor, agent, representative, or other person authorized by Customer to access and use the Services under Customer's Account.
- 1.7. "**Bundle**" means a combination of Products, Modules, functionality, usage rights, or license entitlements offered by Company as a bundle.
- 1.8. "**Customer Data**" means data, files, text, documents, materials, content, information, records, resumes, candidate profiles, job descriptions, contracts, invoices, POs, order forms, prompts, queries, inputs, configurations, workflows, and other information submitted to, uploaded to, transmitted through, stored in, or processed by the Services by or on behalf of Customer or its Authorized Users.
- 1.9. "**Documentation**" means Company's user guides, product documentation, help materials, release notes, technical information, and usage instructions for the Services, as updated from time to time.
- 1.10. "**Fees**" means all amounts payable for Subscriptions, Products, Modules, Bundles, licenses, usage, overages, support, Professional Services, taxes, and other purchases.
- 1.11. "**Module**" means a specific product module, feature set, or role-based component of a Product designed for use by certain functional roles.
- 1.12. "**Order**" means an ordering document, online checkout selection, shopping cart selection, subscription confirmation, in-product subscription modification, invoice, or other ordering process accepted by Company that identifies Products, Modules, Bundles, quantities, pricing, Subscription term, or other commercial terms.
- 1.13. "**Personal Data**" means any information relating to an identified or identifiable natural person, as defined under applicable data protection laws.
- 1.14. "**Product**" means each cloud-based SaaS product made available by Company.
- 1.15. "**Professional Services**" means implementation, configuration, customization, integration, workflow design, training, consulting, data migration, or other professional services provided by Company under a statement of work.

- 1.16. “**Services**” means the Products, Modules, Bundles, AI Features, websites, applications, APIs, support, Documentation, Professional Services, and other services provided by Company.
- 1.17. “**Subscription**” means Customer’s paid or trial-based right to access and use specified Products, Modules, Bundles, or Services for a Subscription term, subject to this Agreement and the applicable Order.
- 1.18. “**Connected Customer**” means another customer of Company that Customer authorizes, approves, connects with, invites, accepts, or otherwise permits to access or interact with certain Customer Data through collaboration, vendor sharing, bench sales, marketplace, search, matching, or similar features of the Product.
- 1.19. “**Public Pages**” means public or semi-public webpages, microsites, job boards, profile pages, talent pages, client attraction pages, or similar pages hosted by Company, including on subdomains such as **jobs.4everi.com**, where certain Customer Data, Public Listing Data, Candidate Summaries, Job Descriptions, or related information may be displayed.
- 1.20. “**Public Listing Data**” means Customer Data that Customer or its Authorized Users submit, configure, designate, publish, approve, or otherwise make available for display on Public Pages or for discovery by Talent, Clients, Connected Customers, vendors, partners, or other permitted third parties. Public Listing Data may include anonymized or summarized candidate information, job descriptions, role requirements, skills, experience summaries, availability, location preferences, rate ranges, employment type, contract type, or similar recruiting-related information.
- 1.21. “**Candidate Summary**” means an anonymized, pseudonymized, redacted, abbreviated, or summarized version of candidate-related Customer Data, which may include skills, experience, job titles, certifications, industry background, availability, work authorization status where lawful, preferred location, rate range, and other recruiting-relevant attributes, but should not include direct identifiers unless Customer has expressly authorized such disclosure.
- 1.22. “**Shared Customer Data**” means Customer Data, Public Listing Data, Candidate Summaries, job description data, vendor list data, bench sales data, staffing requirements, availability information, and related recruiting information that Customer makes available through Public Pages, Connected Customer features, search features, sharing features, or collaboration features.
- 1.23. “**SOW**” means a statement of work or similar document for Professional Services.

2. Scope of Agreement

This Agreement applies to all Products, Modules, Bundles, Subscriptions, trials, purchases, renewals, in-product modifications, Professional Services, and use of the Services.

If there is a conflict among documents, the following order of precedence applies unless expressly stated otherwise:

- 2.1. A signed written agreement between Company and Customer;
- 2.2. The applicable SOW, but only for Professional Services covered by that SOW;
- 2.3. The applicable Order;
- 2.4. The Data Processing Addendum;
- 2.5. This Agreement (Cloud SaaS Terms and Conditions);
- 2.6. Other exhibits, policies, or Documentation incorporated by reference.

3. Access Rights and License

Subject to Customer’s compliance with this Agreement and payment of all Fees, Company grants Customer a limited, non-exclusive, non-transferable, non-sublicensable, revocable right during the applicable Subscription term to allow Authorized Users to access and use the Services solely for Customer’s internal business purposes.

Customer may not use the Services for the benefit of any third party except as expressly permitted in an Order or Documentation.

4. Authorized Users, Licenses, Modules, and Bundles

- 4.1. Authorized Users: Customer is responsible for all access to and use of the Services by Authorized Users and for ensuring that Authorized Users comply with this Agreement.
- 4.2. License Quantities: Customer must purchase and maintain sufficient licenses, seats, quantities, usage rights, or entitlements for all Authorized Users and usage. Unless otherwise stated in an Order, licenses are assigned to named Authorized Users and may not be shared, pooled, or used concurrently by multiple individuals.
- 4.3. Role-Based Modules: Modules may be designed for specific functional roles. Customer is responsible for assigning appropriate Modules to Authorized Users. Company may restrict use of a Module to the intended role or license type.

- 4.4. Bundles: Bundles may include multiple Modules or Products intended for users who perform multiple roles, such as business owners, executives, or leadership teams. Bundle composition, features, and entitlements may vary by plan and may be changed for future purchases or renewals.
- 4.5. Changes to Users and Quantities: Customer may add or remove Authorized Users, Modules, Bundles, or quantities through the Services if enabled. Additional licenses or modules may result in prorated or immediate charges. Reductions may take effect immediately, at the next renewal, billing cycle, or as otherwise stated in the checkout flow or Order.

5. Trials

- 5.1. Trial Period: Company may offer a free or discounted trial for certain Services. Trial availability and duration are determined by Company.
- 5.2. Trial Conversion: Unless otherwise stated during signup or checkout, after the trial period expires, the Subscription will convert to a paid monthly Subscription, and Customer authorizes Company or its payment processor to charge the applicable Fees and taxes using Customer's payment method.
- 5.3. Trial Limitations: Trial Services may be limited, modified, suspended, or terminated at any time. Company may impose usage limits, feature restrictions, data retention limits, or other restrictions during trials.
- 5.4. Trial Data: If Customer does not continue with a paid Subscription after the trial period, Customer is responsible for requesting Company to delete Customer Data. Company may delete trial data after expiration or termination.
- 5.5. No Warranties During Trial: Trial Services are provided "as is" and "as available," without warranties, indemnities, service levels, or support commitments, to the maximum extent permitted by law.

6. Orders, Subscription Changes, and Pricing

- 6.1. Online Checkout: Customer may purchase Products, Modules, Bundles, and license quantities through Company's website shopping cart, checkout pages, or in-product subscription management tools. The unit price and total price may be displayed in the cart or checkout flow. Taxes may be calculated and displayed by the payment processor during checkout.
- 6.2. Subscription Creation: Upon successful checkout, a Subscription will be created for the selected Products, Modules, Bundles, and quantities.
- 6.3. Subscription Modifications: Customer may modify a Subscription, including by adding items, removing items, changing quantities, or changing plans, if enabled in the Services. Company may calculate resulting Fees based on then-current pricing, Customer's current price list, an applicable legacy price list, proration, discounts, promotional terms, or other pricing logic determined by Company.
- 6.4. Pricelist Differences: Customer acknowledges that pricing applicable to an initial Subscription may differ from pricing applicable at the time of later modification, renewal, expansion, downgrade, or reactivation. Unless otherwise expressly stated in an Order, Company may apply then-current pricing to new purchases, added quantities, added Modules, added Bundles, upgrades, renewals, or modifications.
- 6.5. Pricing Changes: Company may change prices, plans, Product packaging, Bundles, Modules, features, and usage limits from time to time. Pricing changes for existing Subscriptions will take effect at renewal or as otherwise permitted under this Agreement, an Order, or applicable law. Company may introduce usage and/or consumption based pricing.
- 6.6. Annual Price Increase: Company may increase Fees of Subscriptions by up to 3% annually, and may also increase Fees to reflect changes in usage, quantities, taxes, third-party costs, inflation, currency fluctuations, new features, Product changes, or other business conditions. If Company increases Fees beyond any committed cap in an applicable Order, Customer's sole remedy is to decline renewal or terminate as permitted in this Agreement.
- 6.7. Promotions and Discounts: Promotions, discounts, trial offers, coupons, and special pricing are discretionary and may be subject to additional conditions. Unless expressly stated otherwise, promotions apply only to the initial term or specified period and do not apply to renewals, expansions, or modifications.

7. Fees, Payment, Taxes, and Billing

- 7.1. Payment Authorization: Customer authorizes Company and its payment processors, to charge Customer's payment method for all Fees, taxes, renewals, Subscription modifications, usage, overages, and other amounts due.
- 7.2. Monthly Billing: Unless otherwise stated in an Order, paid Subscriptions are billed monthly in advance and automatically renew monthly until canceled or terminated.
- 7.3. Taxes: Fees are exclusive of taxes unless expressly stated otherwise. Customer is responsible for all sales, use, VAT, GST, withholding, digital services, and similar taxes, duties, levies, or governmental assessments, excluding taxes based on Company's net income. Taxes may be calculated and collected through a payment processor.
- 7.4. Failed Payments: If payment fails, Company may retry the charge, suspend access, downgrade Services, delete or restrict data, charge late fees where lawful, and pursue collection. Customer is responsible for any chargebacks, bank fees, collection costs, and reasonable attorneys' fees incurred by Company in collecting unpaid amounts.

- 7.5. No Refunds: Except as expressly required by law or stated in an Order, Fees are non-cancelable and non-refundable, including for unused time, unused licenses, unused Modules, or unused features.
- 7.6. Payment Processor Terms: Payments may be processed by third-party payment processors. Customer's use of payment processing may be subject to the payment processor's terms and privacy notice. Company is not responsible for payment processor acts or omissions.

8. Customer Responsibilities

Customer is responsible for:

- 8.1. The accuracy, quality, legality, and appropriateness of Customer Data;
- 8.2. Obtaining all rights, permissions, consents, and notices required to submit and process Customer Data;
- 8.3. Ensuring that resumes, candidate information, job descriptions, contracts, and other Customer Data may lawfully be processed by Company, Cloud Providers, AI Providers, and subprocessors;
- 8.4. Compliance with employment, recruiting, privacy, data protection, anti-discrimination, consumer protection, records retention, and other laws applicable to Customer's use of the Services;
- 8.5. Authorized User activity and credentials;
- 8.6. Maintaining its own backups where appropriate;
- 8.7. Reviewing AI Outputs before use;
- 8.8. Using the Services only for lawful business purposes and in accordance with the Documentation.

If Customer uses Company's Recruiting App, then Customer is also responsible for:

- 8.9. Determining whether Candidate Data, Candidate Summaries, job descriptions, vendor lists, and other recruiting information may be published, displayed, or shared through the Services;
- 8.10. Obtaining candidate consent where required before marketing, publishing, sharing, or submitting candidate profiles;
- 8.11. Ensuring job descriptions and candidate summaries comply with applicable employment, recruiting, anti-discrimination, advertising, and privacy laws;
- 8.12. Reviewing anonymized or summarized candidate information before publication or sharing;
- 8.13. Managing Public Recruiting Page settings and Connected Customer permissions;
- 8.14. Ensuring Customer's Authorized Users do not improperly disclose confidential, sensitive, or personal information;
- 8.15. Honoring candidate opt-out, deletion, correction, access, consent withdrawal, and similar rights where applicable.

9. Restrictions and Acceptable Use

Customer must not, and must not permit any person to:

- 9.1. Copy, modify, translate, reverse engineer, decompile, disassemble, or attempt to derive source code or underlying models of the Services;
- 9.2. Rent, lease, resell, sublicense, distribute, or provide service bureau access to the Services;
- 9.3. Circumvent license limits, usage limits, security controls, or access controls;
- 9.4. Use the Services to develop a competing product or service;
- 9.5. Scrape, harvest, crawl, or extract data except through permitted functionality;
- 9.6. Upload malware, viruses, worms, or malicious code;
- 9.7. Interfere with or disrupt the Services;
- 9.8. Use the Services in violation of applicable laws or third-party rights;
- 9.9. Submit highly sensitive information unless expressly permitted, including government IDs, financial account numbers, health data, biometric data, children's data, or special categories of data, except where Customer has obtained all required consents and has confirmed that the applicable Services are appropriate for such processing;

- 9.10. Use AI Features for unlawful discrimination, automated decision-making without required human review, or employment decisions where prohibited or restricted by law;
- 9.11. Use the Services to generate unlawful, deceptive, defamatory, infringing, harassing, harmful, or discriminatory content;
- 9.12. Attempt to bypass AI safety controls or third-party provider policies;
- 9.13. Misrepresent AI Outputs as human-generated where disclosure is legally required.

Company may suspend or terminate access for violations of this Section.

10. AI Features

- 10.1. Use of AI Providers: Customer acknowledges that certain AI Features use AI Providers accessed through APIs. Customer Data, including resumes, candidate information, job descriptions, contracts, leads, opportunities, prompts, and related materials, may be transmitted to AI Providers and other subprocessors to provide the Services.
- 10.2. AI Inputs and Outputs: Customer Data submitted to AI Features is referred to as “**AI Input**”. Responses, analyses, recommendations, ratings, rankings, generated text, classifications, summaries, and other results returned by AI Features are referred to as “**AI Output**”.
- 10.3. No Guarantee of Accuracy: AI Output may be inaccurate, incomplete, biased, misleading, non-unique, or unsuitable for Customer's intended use. Company does not warrant that AI Output is correct, complete, reliable, lawful, non-infringing, unbiased, or fit for any particular purpose.
- 10.4. Human Review Required: Customer is solely responsible for evaluating AI Output and must use qualified human review before relying on AI Output, especially for employment, recruiting, hiring, promotion, compensation, termination, contracting, legal, compliance, financial, or other material decisions.
- 10.5. Employment and Recruiting Use: If Customer uses the Services to evaluate, match, rate, rank, screen, recommend, or compare candidates, resumes, job descriptions, skills, experience, or qualifications, Customer is solely responsible for compliance with all applicable employment, labor, equal opportunity, anti-discrimination, automated employment decision tool, AI transparency, notice, consent, audit, bias testing, recordkeeping, and similar laws.
- 10.6. Company does not make hiring, employment, or contracting decisions on Customer's behalf.
- 10.7. Third-Party AI Terms: Customer's use of AI Features may be subject to AI Provider terms, policies, usage restrictions, and technical limitations. Customer must not use AI Features in any manner that would violate those terms or policies. Company may modify, suspend, or disable AI Features if required by an AI Provider or applicable law.
- 10.8. AI Provider Changes: Company may change AI Providers, models, configurations, prompts, safety systems, or AI architecture at any time without notice, provided Company does not materially reduce core functionality of paid Services during the then-current Subscription term.
- 10.9. Similar Outputs: Due to the nature of AI systems, AI Output may not be unique, and similar or identical output may be generated for other customers. Customer has no rights in output generated for other customers.
- 10.10. Training and Model Improvement: Company will not intentionally use Customer Data to train Company's general-purpose AI models unless permitted by the applicable Order, Documentation, Privacy Policy, DPA, or Customer's account settings. However, AI Providers may process AI Input and AI Output according to their applicable terms and data processing commitments. Company will use commercially reasonable efforts to configure AI Provider services to limit provider use of Customer Data for model training where such controls are available and commercially reasonable.
- 10.11. AI Exhibit: Additional AI-specific terms are set forth in **Exhibit C, AI Features Terms**, incorporated by reference.

11. Ownership and License to Customer Data

- 11.1. As between the parties, Customer retains all right, title, and interest in Customer Data. Customer grants Company a worldwide, non-exclusive, royalty-free license to host, copy, transmit, process, store, display, publish, distribute, disclose, modify, format, index, summarize, analyze, create technical derivatives of, and otherwise use Customer Data as necessary to:
 - a. Provide, operate, secure, support, maintain, and improve the Services and as otherwise permitted by this Agreement;
 - b. Provide AI Features;
 - c. Process Customer's instructions and configurations;
 - d. Display Public Listing Data on Public Pages;
 - e. Enable candidate marketing, job posting, talent attraction, and client attraction features;
 - f. Enable Connected Customer, bench sales collaboration, vendor list sharing, search, matching, ranking, filtering, recommendation, and marketplace features;
 - g. Comply with applicable law and enforce this Agreement.

Customer represents and warrants that it has all rights, permissions, consents, notices, and lawful bases necessary to grant this license and to allow Company to process, display, publish, share, and disclose Customer Data as contemplated by the Services and this Agreement.

- 11.2.** Aggregated and De-Identified Data: Company may collect and use aggregated, anonymized, or de-identified data derived from use of the Services for analytics, benchmarking, product improvement, research, security, and business purposes, provided such data does not identify Customer or any individual and is not reasonably capable of re-identification.
- 11.3.** Data Retention: Company may retain Customer Data during the Subscription term and for a reasonable period thereafter for backup, archival, audit, legal, tax, security, or legitimate business purposes, unless otherwise stated in the DPA or required by law.
- 11.4.** Data Export: During the Subscription term, Customer may request Company for an export of its data. Following termination, Company may make Customer Data available for export for a limited period at its discretion or as required by law.
- 11.5.** Deletion: After termination or expiration, Company may delete Customer Data according to its standard retention practices, subject to legal obligations, backup retention, dispute resolution, security needs, and the DPA.

12. Customer Data Publication, Sharing and Collaboration

If Customer uses Company's recruiting, staffing, bench sales, vendor collaboration, client attraction, talent attraction, job posting, candidate marketing, Request for Proposal (RFP), Contract Negotiations & eSignatures (CLM), Quoting or related features, Customer acknowledges that the Services may allow Customer and its Authorized Users to publish, display, share, search, transmit, or otherwise make available certain Customer Data to third parties, including Talent, Clients, prospective clients, vendors, partners, Connected Customers, and other users of the Services.

Such features may include:

- a. Public Pages, RFP pages hosted on Company-controlled domains or subdomains, including ****jobs.4everi.com****;
- b. Anonymized or summarized candidate profile displays;
- c. Job description displays or summaries;
- d. Candidate-to-job matching, searching, and filtering;
- e. Bench sales collaboration;
- f. Vendor list sharing;
- g. Customer-to-Customer connection features;
- h. Cross-customer candidate and job search features;
- i. Marketplace, directory, network, or collaboration functionality;
- j. Lead generation, talent attraction, and client attraction functionality.

12.1. Customer Authorization to Publish and Share

Customer authorizes Company to host, copy, process, display, publish, distribute, transmit, disclose, index, make searchable, and otherwise make available Shared Customer Data as configured, enabled, approved, submitted, or permitted by Customer or its Authorized Users through the Services.

This authorization includes Company's right to display Public Listing Data and Data Summaries on Public Pages and to make Shared Data available to Connected Customers and other permitted recipients through collaboration, search, matching, filtering, notification, recommendation, and similar features.

12.2. Public Pages

Customer acknowledges that Public Pages may be accessible by third parties, including search engines, website visitors, prospective candidates, prospective clients, prospective vendors, vendors, partners, and other customers or users, depending on the configuration of the Services.

Customer is solely responsible for determining what Customer Data is appropriate to publish or display on Public Pages. Customer must not publish or authorize publication of candidate information, resume information, job descriptions, RFP information, contract information, confidential information, or Personal Data unless Customer has all rights, permissions, consents, notices, and lawful bases required to do so.

12.3. Anonymized and Summarized Data

The Services may generate or display anonymized, redacted, pseudonymized, abbreviated, or summarized candidate information to help Customer attract Talent, Clients, Vendors, Partners and other entities.

Customer acknowledges that:

- a. Anonymization and summarization may reduce but may not eliminate the risk of re-identification;
- b. Candidate information may still be considered Personal Data under applicable law if it can reasonably be associated with an identifiable individual;
- c. Customer is responsible for reviewing Candidate Summaries and confirming that they are appropriate for publication or sharing;
- d. Customer must not rely solely on automated redaction, anonymization, or summarization where legal compliance requires human review;
- e. Company does not guarantee that any Candidate Summary is fully anonymous, non-identifying, or legally sufficient for Customer's intended use.

12.4. Job Description and Talent Publication and Sharing

Customer authorizes Company to display, publish, summarize, match, index, and make searchable job descriptions, Talent information and related job information submitted by Customer through the Services.

Customer represents and warrants that Customer has the right to publish and share all job descriptions and job-related content submitted to the Services and that such content does not violate any confidentiality obligation, third-party right, employment law, equal opportunity law, advertising law, or other applicable law.

12.5. Connected Customer Features

The Services may allow Customer to connect with other customers using Company Apps. If Customer connects with, invites, approves, accepts, or otherwise enables sharing with a Connected Customer, Customer authorizes Company to make Shared Customer Data available to that Connected Customer according to Customer's settings, selections, permissions, and use of the Services.

Connected Customer features may permit Connected Customers to:

- a. View short summaries of Customer's Candidate Data;
- b. View short summaries of Customer's job descriptions;
- c. Search Customer's shared candidate profiles;
- d. Search Customer's shared job descriptions;
- e. Receive candidate or job recommendations;
- f. Participate in bench sales collaboration;
- g. Access shared vendor lists or vendor-related information;
- h. Communicate or collaborate with Customer through the Services.

12.6. Connected Customer Data Usage Rules

When Customer accesses Shared Customer Data of another customer, Customer agrees that such data is provided solely for legitimate recruiting, staffing, hiring, placement, business development, vendor collaboration, bench sales, or related professional purposes.

Customer must treat non-public Shared Customer Data received from another customer as confidential and must not disclose it except to Customer's personnel, clients, vendors, or representatives who have a legitimate need to know for permitted recruiting or staffing purposes and who are bound by confidentiality or professional obligations.

Customer must comply with all applicable laws when using another customer's Shared Customer Data and must delete or stop using such data upon request by the disclosing customer, the relevant candidate, Company, or as required by law.

Company is not a party to and is not responsible for any separate business relationship, fee arrangement, placement arrangement, vendor agreement, client agreement, candidate agreement, or dispute between customers, Connected Customers, vendors, candidates, or clients.

12.7. Cross-Customer Search

Customer acknowledges that the Services may allow Connected Customers, and potentially other permitted customers depending on product configuration, to search, filter, view, match, or receive summaries of Shared Customer Data.

Customer authorizes Company to index, structure, tag, transform, summarize, analyze, and otherwise process Shared Customer Data to enable search, filtering, matching, ranking, recommendation, AI-assisted discovery, and similar functionality.

12.8. Visibility Settings and Customer Responsibility

The Services may provide settings, permissions, toggles, publication controls, sharing controls, connection controls, or other configuration options. Customer is solely responsible for:

- a. Selecting appropriate visibility settings;
- b. Reviewing data before publication or sharing;
- c. Managing connections with Connected Customers;
- d. Determining which candidates, job descriptions, vendor lists, or other data may be shared;
- e. Removing or unpublishing data when it should no longer be visible;
- f. Ensuring Authorized Users do not publish or share data improperly;
- g. Ensuring shared data remains accurate, current, lawful, and appropriate.

Company is not responsible for Customer's publication, sharing, connection, visibility, or permission decisions.

12.9. Candidate Consent and Notice

Customer represents and warrants that, before submitting, publishing, sharing, or making available candidate-related Customer Data through the Services, Customer has provided all required notices and obtained all required rights, permissions, authorizations, and consents from candidates, employees, contractors, applicants, consultants, or other individuals.

This includes any legally required consent or notice for:

- a. Publishing or marketing candidate profiles;
- b. Sharing candidate information with clients, vendors, staffing partners, or Connected Customers;
- c. Processing candidate information using AI Features;
- d. Using candidate information for matching, ranking, scoring, screening, or recommendations;
- e. Transferring candidate information internationally;
- f. Displaying anonymized, pseudonymized, or summarized candidate information on Public Pages;
- g. Retaining, storing, or reusing candidate information for future opportunities.

Customer further represents that each candidate whose information is submitted to the Services for public posting, client presentation, vendor sharing, bench sales, or Connected Customer collaboration has not opted out of such use, or that Customer has otherwise determined that such processing is legally permitted.

Company may rely on Customer's representations and configurations and has no obligation to independently verify candidate consent, authorization, availability, identity, credentials, or right-to-work status.

12.10. No Responsibility for Third-Party Use After Disclosure

Customer acknowledges that once Shared Customer Data is made available to Public Page visitors, Talent, Clients, Connected Customers, vendors, partners, or other third parties, Company may not be able to control how such recipients use, copy, store, disclose, or further distribute the information.

Company is not responsible for any access, use, disclosure, copying, downloading, retention, re-identification, misuse, or further distribution of Shared Customer Data by third parties, except to the extent caused by Company's breach of this Agreement.

12.11. Connected Customer Conduct

Each customer is responsible for its own use of Shared Customer Data received from another customer. Customer must not, and must ensure its Authorized Users do not:

- a. Use another customer's Shared Customer Data except for legitimate recruiting, staffing, vendor collaboration, bench sales, business development, or related business purposes;
- b. Attempt to re-identify anonymized candidate data except as permitted by the disclosing customer or applicable law;
- c. Scrape, bulk export, harvest, or misuse another customer's data;
- d. Circumvent visibility, access, rate limit, or permission controls;
- e. Use another customer's data for unlawful discrimination, spam, harassment, competitive intelligence, or unauthorized solicitation;
- f. Disclose another customer's non-public Shared Customer Data to unauthorized third parties;
- g. Violate applicable privacy, employment, anti-discrimination, confidentiality, or data protection laws.

12.12. No Endorsement or Verification

Company does not verify and is not responsible for the accuracy, quality, legality, availability, identity, qualifications, credentials, ownership, authorization, or suitability of candidates, job descriptions, vendor lists, customers, Connected Customers, clients, opportunities, summaries, matches, or other Shared Customer Data.

Company's display, search, matching, ranking, or recommendation of Shared Customer Data does not constitute an endorsement, certification, employment recommendation, staffing recommendation, legal opinion, or guarantee.

12.13. Removal and Moderation

Company may remove, disable, restrict, de-index, suspend, or modify access to any Public Listing Data or Shared Customer Data if Company reasonably believes that the data:

- a. Violates this Agreement;
- b. Violates applicable law;
- c. Violates third-party rights;
- d. Contains Personal Data that appears improperly disclosed;
- e. Creates security, privacy, legal, operational, reputational, or commercial risk;
- f. Is inaccurate, misleading, unlawful, discriminatory, offensive, harmful, or inappropriate;
- g. Is required to be removed by a candidate, data subject, regulator, court, platform provider, AI Provider, or other third party.

Company has no obligation to monitor Shared Customer Data but may do so at its discretion.

12.14. Candidate and Third-Party Requests

If Company receives a request from a candidate or other data subject regarding Shared Customer Data, Company may, in its discretion:

- a. Refer the requester to Customer;
- b. Notify Customer;
- c. Remove, restrict, or de-index the relevant data;
- d. Take other action Company reasonably determines is appropriate or legally required.

Customer remains responsible for responding to candidates and other data subjects regarding Customer's recruiting activities and Customer Data.

12.15. Search Engine Indexing

Customer acknowledges that Public Pages and anonymized Talent Pages may be indexed by search engines or archived by third parties unless Company provides and Customer enables settings intended to limit indexing. Company does not guarantee that search engines or third-party archives will remove or update cached content.

12.16. Customer Indemnity for Shared Customer Data

In addition to Customer's indemnity obligations elsewhere in the Agreement, Customer will defend, indemnify, and hold harmless Company, its Affiliates, officers, directors, employees, contractors, vendors, licensors, and agents from and against any claims, damages, liabilities, penalties, fines, losses, costs, and expenses, including reasonable attorneys' fees, arising out of or relating to:

- a. Public Listing Data;
- b. Shared Customer Data;
- c. Candidate Data published, shared, searched, summarized, displayed, or disclosed through the Services;
- d. Job descriptions or job-related content published or shared through the Services;
- e. Vendor list sharing or bench sales collaboration;
- f. Customer's connection with or sharing of data with Connected Customers;
- g. Customer's failure to obtain required candidate consents or provide required notices;
- h. Claims by candidates, employees, contractors, applicants, clients, vendors, Connected Customers, or other third parties relating to Customer's use of Recruiting App sharing features;
- i. Allegations that Customer's use of the Services violated privacy, employment, recruiting, anti-discrimination, consumer protection, confidentiality, or data protection laws.

13. Privacy and Data Protection

Company's processing of Personal Data is governed by:

13.1. Company's Privacy Policy available at https://4everi.com/Privacy-Policy-v3_20.pdf

13.2. The Data Processing Addendum attached as **Exhibit A**;

13.3. Applicable data protection laws.

To the extent Company processes Personal Data on behalf of Customer as a processor or service provider, the DPA applies. To the extent Company processes Personal Data as an independent controller, Company's Privacy Policy applies.

14. Security

Company will implement and maintain commercially reasonable administrative, technical, and physical safeguards designed to protect Customer Data, as further described in **Exhibit B, Security Policy**.

Customer acknowledges that no cloud service, network, system, or data transmission is completely secure, and Company does not guarantee absolute security.

15. Support and Availability

15.1. Support: Company may provide support according to its then-current support policy, Documentation, or applicable Order.

15.2. Maintenance: Company may perform scheduled or emergency maintenance, updates, upgrades, patches, or changes. Company will use commercially reasonable efforts to minimize disruption.

15.3. Service Levels: Unless a separate service level agreement is included in an Order, Company does not provide guaranteed uptime, service credits, or service levels.

16. Product Changes

Cloud SaaS Terms and Conditions (Version 2.10)

Company may modify, enhance, discontinue, repackage, rename, replace, or remove Products, Modules, Bundles, features, AI models, AI Providers, workflows, plans, limits, or Documentation from time to time.

For paid Subscriptions, Company will use commercially reasonable efforts not to materially reduce core functionality during the current paid Subscription term. This does not restrict Company's right to make changes required for security, legal compliance, third-party provider requirements, AI Provider changes, performance, abuse prevention, or technical reasons.

17. Professional Services and SOWs

- 17.1.** SOW Required: Customizations, implementations, integrations, workflow-specific configurations, and other Professional Services will be provided only under an SOW or other written agreement.
- 17.2.** Fees and Expenses: Professional Services fees, payment terms, expenses, assumptions, dependencies, and deliverables will be set forth in the applicable SOW.
- 17.3.** Customer Cooperation: Customer will provide timely access, information, personnel, systems, decisions, approvals, and cooperation reasonably required for Professional Services.
- 17.4.** Deliverables: Unless otherwise stated in an SOW, Company retains ownership of all tools, templates, scripts, know-how, workflows, configurations, methodologies, software, libraries, code, and pre-existing materials used to provide Professional Services. Subject to payment in full, Customer receives a limited right to use deliverables solely with the Services for Customer's internal business purposes.
- 17.5.** Customizations: Customizations may be product configurations rather than bespoke software. Company may use generalized knowledge, ideas, concepts, techniques, and reusable components developed during Professional Services for other customers, provided Company does not disclose Customer's Confidential Information.

18. Confidentiality

- 18.1.** Confidential Information: "Confidential Information" means non-public information disclosed by one party to the other that is marked confidential or should reasonably be understood to be confidential, including business, technical, financial, product, security, pricing, customer, and data information.
- 18.2.** Obligations: The receiving party will use the disclosing party's Confidential Information only to perform under this Agreement and will protect it using reasonable care. The receiving party may disclose Confidential Information to employees, contractors, Affiliates, advisors, and subprocessors who need to know it and are bound by confidentiality obligations.
- 18.3.** Exclusions: Confidential Information does not include information that is publicly available, already known without obligation, independently developed without use of Confidential Information, or rightfully received from a third party without confidentiality obligations.
- 18.4.** Required Disclosure: The receiving party may disclose Confidential Information if required by law, subpoena, or court order, provided it gives prompt notice where legally permitted.

19. Intellectual Property

- 19.1.** Company IP: Company and its licensors retain all right, title, and interest in the Services, Products, Modules, Bundles, AI Features, software, technology, Documentation, workflows, user interfaces, algorithms, models, prompts, templates, designs, know-how, and related intellectual property.
- 19.2.** Feedback: If Customer or Authorized Users provide feedback, suggestions, ideas, improvements, or recommendations, Customer grants Company a worldwide, perpetual, irrevocable, transferable, sublicensable, royalty-free license to use them without restriction or compensation.
- 19.3.** No Implied Rights: No rights are granted except as expressly stated in this Agreement.

20. Third-Party Services

- 20.1.** The Services may interoperate with or depend on third-party services, including AI Providers, cloud hosting providers, payment processors, analytics providers, email providers, identity providers, and integration partners.
- 20.2.** Company is not responsible for third-party services, third-party terms, outages, errors, data processing, security incidents, or changes. Company may suspend integrations or features if third-party services become unavailable, insecure, unlawful, or commercially unreasonable.

21. Suspension

Company may suspend Customer's or any Authorized User's access to the Services immediately if:

- 21.1.** Customer fails to pay Fees;
 - 21.2.** Customer violates this Agreement;
- Cloud SaaS Terms and Conditions (Version 2.10)

- 21.3. Company reasonably believes use of the Services poses a security, legal, operational, or reputational risk;
- 21.4. Suspension is required by law, court order, regulator, Cloud Provider, AI Provider, hosting provider, or other third party;
- 21.5. Customer's use exceeds applicable limits or disrupts the Services.

Company will use commercially reasonable efforts to provide notice and an opportunity to cure where practicable.

22. Term and Termination

- 22.1. Term: This Agreement begins when Customer accepts it and continues until all Subscriptions and SOWs have expired or been terminated.
- 22.2. Subscription Term: Unless otherwise stated in an Order, Subscriptions renew monthly until canceled.
- 22.3. Cancellation: Customer may cancel a Subscription using available subscription management interface or by contacting Company. Unless otherwise stated, cancellation takes effect at the end of the then-current billing period, and no refunds or credits are provided.
- 22.4. Termination for Cause: Either party may terminate this Agreement or an affected Order if the other party materially breaches and fails to cure within 30 days after written notice. Company may terminate immediately for nonpayment, unlawful use, security risk, infringement risk, or violation of acceptable use restrictions.
- 22.5. Effect of Termination: Upon termination or expiration:
 - a. Customer's access rights end;
 - b. Customer must stop using the Services;
 - c. Fees already incurred remain payable;
 - d. Company may delete Customer Data according to its retention practices;
 - e. Sections intended to survive will survive.
- 22.6. Survival: Sections regarding payment obligations, Customer Data retention, confidentiality, intellectual property, disclaimers, indemnities, limitations of liability, dispute resolution, governing law, and general provisions survive termination.

23. Warranties and Disclaimers

- 23.1. Mutual Warranties: Each party represents that it has legal authority to enter into this Agreement.
- 23.2. Customer Warranties: Customer represents and warrants that:
 - a. It has all rights, consents, notices, and lawful bases required for Customer Data processing;
 - b. Customer Data and Customer's use of the Services will not violate law or third-party rights;
 - c. Customer will not use the Services for unlawful discrimination or unlawful automated decision-making;
 - d. Customer will comply with applicable laws.
- 23.3. Disclaimer
 - a. TO THE MAXIMUM EXTENT PERMITTED BY LAW, THE SERVICES, AI FEATURES, TRIAL SERVICES, OUTPUTS, DOCUMENTATION, AND PROFESSIONAL SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE." COMPANY DISCLAIMS ALL WARRANTIES, EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, ACCURACY, AVAILABILITY, SECURITY, AND ERROR-FREE OPERATION.
 - b. COMPANY DOES NOT WARRANT THAT THE SERVICES WILL BE UNINTERRUPTED, SECURE, ERROR-FREE, OR THAT AI OUTPUT WILL BE ACCURATE, COMPLETE, LAWFUL, UNBIASED, NON-INFRINGEMENT, OR SUITABLE FOR CUSTOMER'S PURPOSES.

24. Indemnification

- 24.1. Customer Indemnity: Customer will defend, indemnify, and hold harmless Company, its Affiliates, officers, directors, employees, contractors, licensors, vendors, and agents from and against all claims, damages, liabilities, losses, costs, and expenses, including reasonable attorneys' fees, arising out of or relating to:
 - a. Customer Data;
 - b. Customer's or Authorized Users' use of the Services;
 - c. Customer's violation of this Agreement;
 - d. Customer's violation of law or third-party rights;
 - e. Employment, recruiting, hiring, candidate evaluation, contracting, or personnel decisions;
 - f. Customer's reliance on AI Output;
 - g. Customer's failure to obtain required consents, notices, or lawful bases;

h. Claims by candidates, employees, contractors, applicants, or other individuals relating to Customer's use of the Services.

24.2. Company IP Indemnity: Subject to the limitations in this Agreement, Company will defend Customer against a third-party claim alleging that the paid Services, as provided by Company and used in accordance with this Agreement, directly infringe a U.S. patent, copyright, or trademark, and will pay damages finally awarded or settlement amounts approved by Company.

24.3. Exclusions: Company has no indemnity obligation for claims arising from:

- a. Customer Data;
- b. AI Output;
- c. Customer instructions or configurations;
- d. Use in combination with non-Company products or services;
- e. Modifications not made by Company;
- f. Use after Company provides a workaround or termination notice;
- g. trial, beta, free, or evaluation services;
- h. open-source software;
- i. third-party services or AI Providers.

24.4. Remedies: If Services may infringe, Company may procure continued use, modify or replace the Services, or terminate the affected Services and provide a pro rata refund of prepaid unused Fees for the terminated portion. This Section states Company's entire liability and Customer's exclusive remedy for infringement claims.

24.5. Indemnity Procedure: The indemnified party must promptly notify the indemnifying party, provide reasonable cooperation, and allow the indemnifying party to control the defense and settlement, provided no settlement imposes liability or admission of wrongdoing on the indemnified party without consent.

25. Limitation of Liability

25.1. TO THE MAXIMUM EXTENT PERMITTED BY LAW, COMPANY AND ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, CONTRACTORS, LICENSORS, VENDORS, AND AGENTS WILL NOT BE LIABLE FOR INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, EXEMPLARY, PUNITIVE, OR ENHANCED DAMAGES, OR FOR LOST PROFITS, LOST REVENUE, LOST BUSINESS, LOSS OF GOODWILL, LOSS OF DATA, BUSINESS INTERRUPTION, PROCUREMENT OF SUBSTITUTE SERVICES, OR COSTS OF COVER, EVEN IF ADVISED OF THE POSSIBILITY.

25.2. TO THE MAXIMUM EXTENT PERMITTED BY LAW, COMPANY'S TOTAL AGGREGATE LIABILITY ARISING OUT OF OR RELATING TO THIS AGREEMENT WILL NOT EXCEED THE FEES PAID BY CUSTOMER TO COMPANY FOR THE SERVICES GIVING RISE TO THE CLAIM IN THE THREE MONTHS BEFORE THE EVENT GIVING RISE TO LIABILITY.

25.3. FOR TRIAL, FREE, BETA, OR EVALUATION SERVICES, COMPANY'S TOTAL LIABILITY WILL NOT EXCEED USD \$100.

25.4. THE LIMITATIONS APPLY REGARDLESS OF LEGAL THEORY, INCLUDING CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY, WARRANTY, STATUTE, OR OTHERWISE.

26. Export, Sanctions, and Anti-Corruption

26.1. Customer must comply with all applicable export control, sanctions, anti-corruption, and anti-bribery laws. Customer represents that it is not located in, organized under the laws of, or ordinarily resident in any embargoed or sanctioned jurisdiction and is not a restricted party.

26.2. Customer must not use the Services for prohibited end uses, including military, nuclear, chemical, biological, missile, surveillance, or other restricted uses where prohibited by law.

27. Changes to this Agreement

27.1. Company may update this Agreement from time to time by posting an updated version, providing notice in the Services, sending email notice, or otherwise notifying Customer.

27.2. Changes become effective on the stated effective date. For existing paid Subscriptions, material adverse changes will take effect at renewal unless required sooner for legal, security, operational, AI Provider, Cloud provider or compliance reasons.

27.3. Continued use of the Services after changes become effective constitutes acceptance.

28. Notices

28.1. Company may provide notices by email, in-product notification, posting on its website, or other reasonable means. Customer notices to Company must be sent to legal.notice@4everi.com:

28.2. Legal notices are effective upon receipt, except email notices are effective when sent unless the sender receives a delivery failure notice.

29. Governing Law and Venue:

Cloud SaaS Terms and Conditions (Version 2.10)

- 29.1.** This Agreement and any dispute arising out of or related to it will be governed by and construed in accordance with the laws of the State of California, without regard to its conflict of law principles. Each party irrevocably consents and submits to the exclusive personal jurisdiction and venue of the state and federal courts located in Alameda County, California for the resolution of any such dispute.
- 29.2.** Class Action Waiver. To the maximum extent permitted by law, disputes must be brought only on an individual basis and not as a class, collective, consolidated, or representative action.

30. General Terms

- 30.1.** Assignment: Customer may not assign this Agreement without Company's prior written consent. Company may assign this Agreement to an Affiliate or in connection with a merger, acquisition, reorganization, financing, sale of assets, or change of control.
- 30.2.** Subcontractors: Company may use subcontractors, vendors, AI Providers, cloud providers, and other subprocessors to provide the Services. Company remains responsible for its obligations under this Agreement, subject to the limitations herein.
- 30.3.** Force Majeure: Company is not liable for delay or failure caused by events beyond its reasonable control, including acts of God, natural disasters, war, terrorism, labor disputes, internet or utility failures, cyberattacks, governmental actions, epidemics, supply chain failures, or third-party provider outages.
- 30.4.** Government Use: The Services are commercial products developed at private expense. If Customer is a government entity, access is provided only with the rights customarily provided to commercial customers and as restricted by this Agreement.
- 30.5.** Independent Contractors: The parties are independent contractors. This Agreement does not create a partnership, joint venture, agency, fiduciary, or employment relationship.
- 30.6.** Beta Features: Company may offer beta, preview, experimental, pilot, or evaluation features. Beta features may not be optional, may be modified or discontinued at any time, may be subject to additional terms, and are provided "as is" without warranties, support, service levels, or indemnities.
- 30.7.** Severability: If any provision is unenforceable, it will be modified to the minimum extent necessary to make it enforceable, and the remaining provisions remain in effect.
- 30.8.** Waiver: Failure to enforce a provision is not a waiver.
- 30.9.** Entire Agreement: This Agreement is the entire agreement between the parties regarding the Services and supersedes prior or contemporaneous agreements on the same subject.
- 30.10.** No Third-Party Beneficiaries: Except for Company's Affiliates, officers, directors, employees, contractors, licensors, vendors, and agents entitled to protections under this Agreement, there are no third-party beneficiaries.
- 30.11.** Language: This Agreement is drafted in English. Any translation is provided for convenience only, and the English version controls.

EXHIBIT A

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") forms part of the Agreement between Company and Customer.

1. Scope

This DPA applies where Company processes Personal Data on behalf of Customer in providing the Services.

2. Roles

For Personal Data processed on behalf of Customer:

- Customer is the controller/business;
- Company is the processor/service provider;
- Authorized Users and data subjects may include candidates, employees, contractors, applicants, customers, vendors, and other individuals.

For account administration, billing, security, product analytics, and legal compliance, Company may act as an independent controller.

3. Processing Details

- 3.1. Subject Matter: Provision of cloud SaaS Products, AI Features, support, hosting, storage, analytics, and Professional Services.
- 3.2. Duration: For the term of the Agreement and any retention period.
- 3.3. Nature and Purpose: Hosting, storing, transmitting, analyzing, matching, summarizing, extracting, generating, rating, ranking, configuring, supporting, securing, maintaining, and improving the Services.
- 3.4. Categories of Data Subjects: Candidates, job applicants, employees, contractors, recruiters, hiring managers, customer personnel, authorized users, contract parties, and other individuals whose data is included in Customer Data.
- 3.5. Categories of Personal Data: Names, contact information, resumes, work history, education, skills, certifications, job preferences, interview notes, job descriptions, contract information, identifiers, account data, usage logs, and other data submitted by Customer.
- 3.6. Sensitive Data: Customer must not submit sensitive data unless permitted by the Services and lawful. Sensitive data may include demographic data, government IDs, health data, disability status, race, ethnicity, union membership, criminal history, or other special categories if included in resumes or candidate materials.

4. Customer Instructions

Company will process Personal Data only according to Customer's documented instructions, including this Agreement, Orders, Documentation, and Customer's use of the Services, unless required by law.

5. Customer Obligations

Customer is responsible for:

- 5.1. Providing all required notices;
- 5.2. Obtaining all required consents;
- 5.3. Establishing a valid lawful basis for processing;
- 5.4. Responding to data subject requests;
- 5.5. Ensuring Customer Data is accurate and lawful;
- 5.6. Conducting required impact assessments, AI assessments, or bias audits;
- 5.7. Ensuring use of the Services complies with employment and privacy laws.

6. Company Obligations

Company will:

- 6.1. Process Personal Data according to Customer instructions;
- 6.2. Ensure personnel authorized to process Personal Data are bound by confidentiality obligations;
- 6.3. Implement reasonable security measures;
- 6.4. Assist Customer with data subject requests where reasonably possible;
- 6.5. Assist with security incident notifications as required by law;
- 6.6. Delete or return Personal Data after termination as described in the Agreement;
- 6.7. make available information reasonably necessary to demonstrate compliance, subject to confidentiality and security limitations.

7. Subprocessors

- 7.1. Customer authorizes Company to use subprocessors, including cloud hosting providers, AI Providers, payment processors, analytics providers, support providers, email providers, and infrastructure vendors.
- 7.2. Company will provide a list of subprocessors upon request. Company may add or replace subprocessors. Customer may object to a new subprocessor on reasonable data protection grounds within 10 days after notice, and Company may provide a workaround or terminate affected Services.

8. AI Providers as Subprocessors

- 8.1. Customer authorizes Company to transmit AI Input and receive AI Output from AI Providers as necessary for AI Features. AI Providers may process Personal Data in accordance with their applicable data processing terms.
- 8.2. Company will use commercially reasonable efforts to select AI Providers that provide reasonable confidentiality, security, and data protection commitments.

9. International Transfers

- 9.1. Customer authorizes Company and subprocessors to process Personal Data globally where they maintain operations or infrastructure.
- 9.2. For transfers subject to GDPR, UK GDPR, Swiss FADP, or similar laws, the parties will use an appropriate transfer mechanism, which may include:
 - a. EU Standard Contractual Clauses;
 - b. UK International Data Transfer Addendum;
 - c. Swiss amendments;
 - d. Adequacy decisions;
 - e. Other lawful mechanisms.
- 9.3. The applicable Standard Contractual Clauses are incorporated by reference where required.

10. Security Incidents

- 10.1. Company will notify Customer without undue delay after becoming aware of a confirmed unauthorized access, disclosure, alteration, or destruction of Customer Personal Data in Company's control.
- 10.2. Notification will include information reasonably available to Company. Company's notification is not an admission of fault or liability.

11. Data Subject Requests

- 11.1. If Company receives a request from a data subject relating to Customer Personal Data, Company may direct the requester to Customer. Customer is responsible for responding. Company will provide reasonable assistance where required and technically feasible.

12. Deletion and Return

- 12.1. Upon termination, Company will delete Customer Personal Data according to the Agreement and standard retention practices, unless retention is required by law, backup processes, security, dispute resolution, or legitimate business purposes.

13. CCPA/CPRA Service Provider Terms

To the extent California privacy law applies and Company acts as a service provider or contractor, Company will not:

- a. Sell or share Customer Personal Data;
- b. Retain, use, or disclose Customer Personal Data except for business purposes under the Agreement;
- c. Combine Customer Personal Data with personal data from other sources except as permitted by law;
- d. Process Customer Personal Data outside the business relationship except as permitted by law.

14. Audits

- 14.1. Upon reasonable written request, Company will provide security summaries, certifications, questionnaires, or other information reasonably necessary to demonstrate compliance. On-site audits are not permitted unless legally required and must be subject to reasonable scope, confidentiality, timing, and security restrictions.

15. Recruiting App Publication and Sharing Instructions

- 15.1. Customer Instructions for Publication and Sharing: Where Customer uses Recruiting App features to publish, display, share, search, or make available Customer Personal Data, including candidate-related information, job-related information, or vendor-related

information, Customer's use of those features constitutes Customer's documented instruction for Company to process and disclose such Personal Data as configured by Customer. This may include disclosure to:

- a. Public Recruiting Page visitors;
- b. Talent;
- c. Clients and prospective clients;
- d. Vendors and staffing partners;
- e. Connected Customers;
- f. Other permitted users of the Services;
- g. Search, matching, AI, hosting, analytics, and infrastructure subprocessors.

15.2. Controller Responsibility

Customer is the controller or business responsible for determining whether candidate-related Personal Data may be published, shared, disclosed, searched, matched, or otherwise made available through the Services.

Customer is responsible for providing required notices, obtaining required consents, identifying a lawful basis, honoring data subject rights, and complying with employment, recruiting, privacy, AI, and anti-discrimination laws.

15.3. Company Role

Company processes Personal Data according to Customer's instructions when hosting, publishing, sharing, searching, displaying, summarizing, or transmitting Customer Personal Data through the Recruiting App.

However, Company may act as an independent controller for limited purposes described in the Agreement and Privacy Policy, including account administration, billing, security, fraud prevention, service analytics, legal compliance, and protection of Company's rights.

15.4. Public Disclosure Risk

Customer acknowledges that Personal Data published or shared through Public Pages or with Connected Customers may be accessed, copied, stored, indexed, re-disclosed, or otherwise used by third parties. Customer is responsible for determining whether such disclosure is lawful and appropriate.

15.5. Candidate Requests Relating to Shared Data

Customer is responsible for responding to candidate and data subject requests relating to Customer's publication or sharing of candidate-related Personal Data. Company will provide reasonable assistance where required by applicable data protection law and technically feasible.

EXHIBIT B

SECURITY POLICY

Company will maintain a commercially reasonable information security program designed to protect Customer Data.

1. Administrative Safeguards

Company's security program may include:

- a. Security policies and procedures;
- b. Employee confidentiality obligations;
- c. Role-based access controls;
- d. Security awareness practices;
- e. Vendor and subprocessor review;
- f. Incident response procedures;
- g. Periodic risk assessments.

2. Technical Safeguards

Company will use commercially reasonable technical safeguards, which may include:

- a. Encryption in transit using TLS or equivalent;
- b. Encryption at rest where supported by hosting infrastructure;
- c. Authentication controls;
- d. Access logging;
- e. Least-privilege access;
- f. Network and application security controls;
- g. Vulnerability management;
- h. Backup and recovery procedures;
- i. Monitoring for suspicious activity.

3. Physical Safeguards

Company relies on reputable cloud hosting providers for physical data center security. Such providers generally maintain physical access controls, environmental controls, redundancy, and monitoring.

4. Customer Security Responsibilities

Customer is responsible for:

- a. Maintaining secure Authorized User credentials;
- b. Enabling MFA where available;
- c. Managing user access and offboarding;
- d. Securing Customer systems and integrations;
- e. Reviewing account activity;
- f. Using appropriate configurations;
- g. Avoiding unnecessary upload of sensitive data.

5. Incident Response

Company will investigate suspected security incidents and take reasonable steps to contain, mitigate, and remediate confirmed incidents.

6. No Absolute Security

Company does not guarantee that unauthorized third parties will never defeat security measures.

EXHIBIT C

ARTIFICIAL INTELLIGENCE (AI) FEATURES TERMS

These AI Features Terms apply to all AI Features.

1. Customer Control and Responsibility

Customer controls the AI Input submitted to the Services and is responsible for determining whether AI Features are appropriate for Customer's use case.

2. Candidate Matching and Rating

Where AI Features compare a candidate resume to a job description and provide a match score, skills rating, summary, recommendation, or similar analysis:

- a. The output is informational only;
- b. It is not a hiring decision;
- c. Customer must conduct independent human review;
- d. Customer must not rely solely on AI Output for employment decisions;
- e. Customer is responsible for validating job-relatedness, fairness, accuracy, and legal compliance.

3. No Professional Advice

AI Output is not legal, employment, HR, compliance, financial, tax, medical, or professional advice. Customer should consult qualified professionals where appropriate.

4. AI Limitations

AI systems may:

- a. Hallucinate or fabricate facts;
- b. Misinterpret resumes, contracts, or job descriptions;
- c. Produce biased or discriminatory results;
- d. Omit relevant information;
- e. Generate inconsistent results;
- f. Produce non-unique or similar output for different users;
- g. Reflect limitations of training data, prompts, or model behavior.

5. Prohibited AI Uses

Customer must not use AI Features for the following reasons:

- a. To make fully automated employment decisions where prohibited;
- b. To discriminate unlawfully;
- c. To infer sensitive traits where prohibited;
- d. To generate deceptive or fraudulent content;
- e. To violate AI Provider policies;
- f. To process data Customer is not authorized to process;
- g. For high-risk uses without legally required assessments, notices, audits, and human oversight.

6. AI Provider Terms

AI Features may be subject to AI Provider policies. Company may disable or restrict AI Features if Customer's use violates AI Provider terms or poses risk.

7. AI Output Ownership

As between Company and Customer, and subject to this Agreement, Customer may use AI Output generated from Customer's AI Input for Customer's internal business purposes. Company does not represent that AI Output is protectable by intellectual property rights or exclusively owned by Customer.

EXHIBIT D

PROFESSIONAL SERVICES TERMS

1. SOWs

Professional Services will be described in an SOW. Each SOW should include but not limited to:

- a. Scope;
- b. Deliverables;
- c. Timeline;
- d. Fees;
- e. Expenses;
- f. Assumptions;
- g. Customer responsibilities;
- h. Acceptance criteria, if any;
- i. Change control process.

2. Change Orders

Changes to scope, timeline, deliverables, or assumptions require a written change order or other written approval by both parties.

3. Acceptance

Unless otherwise stated in an SOW, deliverables are deemed accepted upon delivery unless Customer provides specific written rejection within 5 business days. Rejections must identify material nonconformities with the SOW.

4. Delays

Company is not responsible for delays caused by Customer, third parties, unavailable systems, inaccurate information, or changed requirements.

5. Ownership

Company retains ownership of pre-existing materials, tools, templates, methods, scripts, code, configurations, APIs, integrations, know-how, and generic components. Customer receives a limited right to use deliverables with the Services after payment.

6. No Work Made for Hire

Unless expressly stated in a signed SOW, deliverables are not "works made for hire."

EXHIBIT E

SUPPORT POLICY

1. Support Channels

Support may be provided through email, in-product support, help desk, chat, documentation, or other channels designated by Company.

Support email: support.me@4everi.com

2. Support Hours

Standard support hours are 9 am to 5 pm PST, excluding Company holidays.

3. Support Scope

Support includes reasonable assistance with:

- a. Account access issues;
- b. Product functionality questions;
- c. Error reports;
- d. Basic configuration questions.

Support does not include:

- a. Custom development;
- b. Customer network or device troubleshooting;
- c. Third-party systems;
- d. Data cleanup;
- e. Legal, HR, compliance, or recruiting advice;
- f. Training beyond standard documentation unless purchased.

4. Response Targets

Unless otherwise stated in an Order, response times are targets only and not guarantees.

Priority	Description	Target Initial Response
P1	Critical production outage affecting all users	8 business hours
P2	Major issue affecting material functionality	3 business day
P3	Minor issue or workaround available	5 business days
P4	General question or enhancement request	3 business days

EXHIBIT F

ACCEPTABLE USE POLICY

Customer and Authorized Users must not use the Services to:

- a. Violate laws or regulations;
- b. Infringe intellectual property, privacy, publicity, or contractual rights;
- c. Upload malware or malicious code;
- d. Attempt unauthorized access;
- e. Disrupt or overload the Services;
- f. Send spam or unsolicited messages;
- g. Process unlawful or improperly obtained data;
- h. Generate or distribute harmful, deceptive, defamatory, or discriminatory content;
- i. Conduct unlawful surveillance or profiling;
- j. Circumvent security, rate limits, or usage controls;
- k. Use the Services for weapons, illegal activities, exploitation, or human rights abuses;
- l. Use AI Features in violation of applicable AI Provider policies.

Company may remove content, suspend access, or terminate Services for violations.