ACCEPTABLE USE POLICY

Visibility HR, LLC · Effective January 1, 2027

This Acceptable Use Policy (the "Acceptable Use Policy") is part of the Subscription Agreement between Client and Visibility HR, LLC or, for a Client on an earlier agreement, that agreement (in either case, the "Agreement"). If this Acceptable Use Policy conflicts with the Agreement, the Agreement controls unless this Acceptable Use Policy expressly provides otherwise. Capitalized terms not defined here have the meanings given in the Agreement.

1. PROPER USE

Client shall, and shall ensure that its Users, comply with this Acceptable Use Policy, the Agreement, and the Documentation. Visibility may deny Client or any User use of the Subscription as required for Visibility to exercise its rights and obligations under, or otherwise enforce, this Acceptable Use Policy or the Agreement. Visibility shall use commercially reasonable efforts to give Client advance notice of any denial of use, where practicable and not harmful to the legitimate interests of Visibility and its Affiliates.

2. RESTRICTIONS

Except as expressly permitted, Client shall not: (i) copy or reproduce the Subscription in any form or medium; (ii) modify, reverse engineer, decompile, adapt, restructure, rearrange, reorganize, recompile, reformat, create derivative works of, change, or add to the Subscription, or attempt to reconstruct or discover any source code or algorithms of the Subscription, by any means; (iii) remove any copyright, proprietary rights, or restrictive legends, or bypass or disable any protections against unlicensed use of the Subscription or third-party data; (iv) remove Visibility's, its Affiliates', or its licensors' legends and notices on any permitted copies, adaptations, and rearrangements of the Subscription; (v) provide or otherwise make the Subscription available to any third party; (vi) fail to take appropriate action with its employees, agents, and subcontractors, by agreement or otherwise, to satisfy its obligations under this Acceptable Use Policy or the Agreement with respect to the use, copying, protection, and security of the Subscription and Client Data; (vii) engage in any use, including copying, modification, redistribution, publication, display, performance, or retransmission, of any portion of the Subscription other than as expressly permitted by the Agreement, without Visibility's prior written consent; or (viii) use the Subscription to send messages that violate applicable laws, rules, or regulations.

3. PROHIBITED USES

Client shall not use the Subscription to knowingly: (i) impersonate any person or entity or misrepresent an affiliation with any person or entity; (ii) intercept any data not intended for Client or its Users; or (iii) perform any hack (ethical or otherwise), including probing, scanning, load testing, penetration testing, or other testing of the security or vulnerability of the Subscription, or otherwise breach security or authentication measures. Client shall not use the Subscription to knowingly upload, post, email, transmit, store, distribute, or otherwise make available: (a) any content, or engage in any conduct, that is unlawful, harmful, untrue, threatening, abusive, harassing, tortious, defamatory, vulgar, obscene, libelous, fraudulent, deceptive, invasive of another's privacy, hateful, racist, or otherwise objectionable; (b) any unsolicited or unauthorized messaging (as further described in Section 8); (c) any Client Data, or material support or resources, to any person or organization designated by the United States government as a foreign terrorist organization or otherwise in violation of U.S. export control or sanctions restrictions; (d) any time bomb, worm, virus, malware, ransomware, lock, drop-dead device, or similar component intended to damage, destroy, alter, or adversely

affect the operation of the Subscription or any related software, hardware, or service, or to reveal, damage, or alter any Client Data or any other person's software, hardware, or information; or (e) any Client Data that Client knows to be incorrect or misleading.

4. LIMITATIONS

Except as otherwise stated in the applicable Order Form or statement of work, Visibility may establish, as described in its Documentation, general practices and limits concerning Client's use of Client Data and the Subscription, including: (i) the maximum number of days that Client Data will be actively retained by or made available through the Subscription; (ii) the maximum number of uploads, posts, or transmissions that may be sent or received through the Subscription; (iii) the maximum size of Client Data, individually or collectively, that may be sent or received through the Subscription; (iv) the maximum storage space allotted to Client; (v) the length of time before an inactive User is automatically logged off; and (vi) the maximum number of times, and the maximum duration for which, Client or its Users may access the Subscription in a given period. Visibility shall give Client commercially reasonable notice of any new practice or limit, which may include notice by update to the publicly available Documentation in accordance with the Agreement. If Client gives Visibility written notice of an objection within fifteen (15) days after receiving notice, the practice or limit will not take effect for Client until the Parties reach agreement. If the Parties cannot reach agreement within sixty (60) days after Client's objection, the practice or limit will not apply to Client for the remainder of the then-current Subscription Period.

5. NAMED USERS

Client shall ensure that only named Users access or use the Subscription and that each named User is a unique person. There is no limit on the number of named Users unless the Order Form states one. Use of a non-Visibility intermediate user interface, portal, or page to aggregate data, information, or actions from multiple individuals into the Subscription will be treated as use by separate named Users. Sharing of usernames or passwords for access to the Subscription is prohibited, and Client is responsible for any misuse of its Users' usernames or passwords.

6. CONSENTS AND AUTHORIZATIONS

Client acknowledges and agrees that: (i) Visibility is not a covered entity or a business associate for purposes of the U.S. Health Insurance Portability and Accountability Act of 1996 and its regulations ("HIPAA"); (ii) Visibility does not act as Client's agent; (iii) Client may use the Subscription to collect and store health-related information about its own job applicants, employees, and other workers that Client needs as an employer for hiring, onboarding, credentialing, and training, such as immunization records, health screening and test results, and fitness-for-duty clearances ("Employment Health Information"); Client is solely responsible for its legal basis for collecting Employment Health Information, for any required notices and consents, for complying with any law that requires such information to be kept confidential or separate from other personnel records, and for limiting access to it to authorized personnel; (iv) Client shall not, and shall ensure each User does not, use the Subscription to store patient records, to perform treatment, payment, health plan, or other health care functions, or to submit any health information that Client holds in its capacity as a health care provider or health plan rather than as an employer; and (v) Client is solely responsible for determining the form of, and providing or obtaining, any notices, consents, and authorizations required by applicable law for the use or disclosure of Client Data. Client understands that the technical processing and transmission of the Subscription, including account information and Client Data, may involve: (a) transmissions over various networks and processing by Visibility and its Subprocessors in the locations described in the Privacy Statement and, where it applies, the Data Processing Addendum; (b) changes to

conform and adapt to the technical requirements of connecting networks or devices; and (c) other transmission or tracking requirements, including the use of cookies as described in the Privacy Statement. Client agrees to permit these transmissions and changes, to obtain any necessary consent from its Users, and to obtain all rights necessary to share, provide access to, and permit use of Client Data by Visibility and its Subprocessors in accordance with the Privacy Statement, the Security Overview, and, where it applies, the Data Processing Addendum.

7. PROFESSIONAL SERVICES

Forms provided to Visibility by Client for onboarding development must be in Microsoft Word format. Additional professional services charges apply if forms are provided in other formats, and those services must be authorized by Client in writing through a new Order Form before they begin. No data feed services are included by default; all feeds must be scoped as additional professional services.

8. EMAIL MESSAGE COMPLIANCE

Client shall comply with the following when sending email messages through the Subscription: (i) use only permission-based marketing email lists, in which each recipient has expressly opted in to receive email messages from Client; (ii) include a working unsubscribe mechanism in each marketing email message that allows the recipient to opt out, except as otherwise required or permitted by applicable law; (iii) honor requests from recipients to be removed from email lists within ten (10) days of receipt or any shorter deadline under applicable law; (iv) maintain, publish, and comply with a privacy policy that meets all applicable legal requirements, whether or not Client controls the sending of the email message; and (v) include in each email message a link to a current privacy policy applicable to that message and a valid physical mailing address or a link to it. While using the Subscription, Client shall not: (1) send email messages to addresses obtained from purchased or rented lists; (2) use third-party email addresses, domain names, or mail servers without proper permission; (3) routinely send email messages to non-specific addresses (for example, webmaster@domain.com or info@domain.com); (4) send email messages that result in an unreasonable number of spam or similar complaints; (5) disguise the origin or subject matter of any email message or falsify or manipulate the originating address, subject line, header, or transmission path information; (6) send offers for the purpose of obtaining personal information or generating leads for third parties; (7) send chain letters, pyramid schemes, or other messages that encourage the recipient to forward the content to strangers; (8) send to lists of addresses that are programmatically generated or scraped from the internet; (9) employ sending practices, or have overall message delivery rates, that adversely affect the Subscription; or (10) import into any contact list uploaded to the Subscription any Social Security numbers, national insurance numbers, payment card data, passwords, security credentials, bank account numbers, or sensitive personal, health, or financial information of any kind. Other terms may apply to Client's use of messaging services, as described in Section 9.

9. PHONE NUMBER PROVIDERS (IF APPLICABLE)

Some messaging services may enable Client to send messages through a phone number or short code using SMS or other methods. Visibility engages third-party vendors to provide the phone numbers and short codes that Client uses through those services. Client's use of phone numbers and short codes within the Subscription must comply with the guidelines of the CTIA (Cellular Telecommunications Industry Association), the CWTA (Canadian Wireless Telecommunications Association), the ETNO (European Telecommunications Network Operators' Association), and the GSMA (GSM Association), as applicable. If Client subscribes to a messaging service, Client is solely responsible for complying with all applicable terms, conditions, guidelines, and policies.

10. DATA IMPORT AND EXPORT

Client Data for legacy data migration and systems integration must be provided by Client, or a third party authorized by Client, to Visibility in Microsoft Excel format. If Client asks Visibility to update Client Data in the Subscription using the import tool, Client shall pre-screen the Client Data for accuracy, integrity, completeness, and quality before making it available to Visibility. Visibility can perform a full system restoration, at its then-current fees, only from the most recent data backup taken before the modification or deletion of the Client Data; any actions taken after that backup, including job, candidate, or hiring manager profiles created after it, will be lost. Client must report Client Data loss or corruption to Visibility within seven (7) days; failure to do so may prevent Visibility from fully restoring Client's Subscription to an uncorrupted state.

Use of unsecure FTP channels reduces the security measures that protect Client Data in transfer. If Client chooses to use an unsecure FTP channel to transfer Client Data to or from Visibility, Client shall encrypt all Client Data with PGP encryption before transfer. Client's use of unsecure FTP channels or other third-party services (for example, Google Drive or Box) to transfer, import, or export Client Data to or from Visibility is at Client's own risk, and Visibility has no liability arising out of or in connection with that use.