

Effective Date: 11/03/2020

Ascentis Terms of Use

Ascentis Corporation, and its subsidiaries and affiliates, including, but not limited to NOVAtime Technology, Inc., (collectively “ASC,” “we,” “us,” and “our”) is a leading provider of easy-to-use human capital management and workforce management products and services.

You agree that the following Terms of Use and our Privacy Policy shall apply to the commercially available versions of our workforce management and human capital management Software-as-a-Service (“SaaS”) solutions, the services related thereto and your use of equipment (including, but not limited to, timeclocks, badges, beacons, and beacon readers) rented or sold by us or our partners (collectively, “Solutions”).

Acceptance. By accessing and using our Solutions, or by clicking “I Accept” when signing up for a user account, you acknowledge that you have read, understood, and agree to be bound by these Terms of Use and the Privacy Policy referenced herein. If you do not accept these Terms of Use and the Privacy Policy, you are not authorized to use the Solutions. We may make modifications to the foregoing at any time and such modification will be effective upon its posting to this website. Your continued use of the Solutions, after any modifications to these Terms of Use shall indicate your agreement with such modified terms.

Site Content. The Solutions contain material, such as software, text, graphics, images, video, audio and other material (collectively referred to as the “Content”). The Content may be owned by us or may be provided through an arrangement we have with others, including other users of the Solutions, our service providers and their partners, sponsors, or affiliates. The Content is protected by copyright under both United States and foreign laws and may not be modified or altered in any way. Unauthorized use of the Content may violate copyright, trademark, and other laws. You have no rights in or to the Content, and you may not use the Content except as specifically provided in these Terms of Use.

Permitted Use. The Solutions are for personal use in conjunction with your job duties only, and may not be used in connection with any other commercial endeavors except those that are specifically approved by us. The following activities are expressly prohibited: (i) collecting usernames and/or email addresses of other users by electronic or other means for the purpose of sending unsolicited email or other communications; (ii) any use of the Solutions which in our sole judgment, degrades the reliability, speed, or operation of the Solutions or any underlying hardware or software thereof, and (iii) any use of the Solutions which is unlawful or in violation of these Terms of Use.

You may not access or utilize the Solutions in any manner that could damage, disable, overburden, or impair any of our accounts, computer systems or networks. You may not attempt to gain unauthorized access to any parts of the Solutions, computer systems or networks. You may not use any robot, spider, scraper, or other automated means to access the Solutions, computer systems or networks.

You may not access, download, use, or export the Content provided on the Solutions, in

violation of U.S. export laws or regulations, or in violation of any other applicable laws or regulations. Your use of the Solutions is subject to termination at any time in our sole discretion.

Password Protection. Access to, and use of, password protected areas of the Solutions is restricted to authorized users only and you may not share your password(s), account information, or access to the Solutions. You are responsible for maintaining confidentiality of your passwords and account information, and you are responsible for all activities that occur under your password(s) or account(s) or as a result of your access to the Solutions. You agree to notify us immediately of any unauthorized use of your password(s) or account(s).

Biometric Data

If you use the biometric scanning feature on one of our timeclocks (which may include, but is not limited to, scanning your fingerprint, handprint, or face), we may create data using a mathematical algorithm based off of your biometric feature ("Biometric Data") and store that Biometric Data at a site controlled by your employer or in a cloud environment controlled by us. By clicking "I Accept" when signing up for a user account, clicking "OK" or "NEXT" when enrolling yourself in our timeclock, or by using the Solutions, you permit us to create, store, and use the Biometric Data associated with you.

We have put industry standard measures in place to protect the Biometric Data. We only use the Biometric Data for identity verification, workplace security, and fraud prevention purposes. We only store the Biometric Data for so long as you continue to use the Solutions, or until your employer asks us to delete the Biometric Data. In no cases is the Biometric Data stored for more than one year after you have stopped using the Solutions.

For more information, please see our [Biometric Data Notice](#).

NO WARRANTIES. CONTENT PROVIDED ON THE SOLUTIONS, AND THE SOLUTIONS THEMSELVES, ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. WE USE REASONABLE EFFORTS TO INCLUDE ACCURATE AND UP-TO-DATE INFORMATION ON THE SOLUTIONS. WE DO NOT, HOWEVER, MAKE ANY WARRANTIES OR REPRESENTATIONS AS TO THEIR ACCURACY OR COMPLETENESS. ASC PERIODICALLY ADDS, CHANGES, IMPROVES, OR UPDATES THE SOLUTIONS AND THEIR CONTENTS WITHOUT NOTICE. WE DO NOT ASSUME ANY LIABILITY OR RESPONSIBILITY FOR ANY ERRORS OR OMISSIONS IN THE CONTENT OR THE SOLUTIONS. YOUR USE OF THE SOLUTIONS IS AT YOUR OWN RISK.

LIMITATION OF LIABILITY. UNDER NO CIRCUMSTANCES SHALL WE BE LIABLE FOR ANY DAMAGES SUFFERED BY YOU, INCLUDING ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, ANY LOST PROFITS OR DAMAGES FOR BUSINESS INTERRUPTION, LOSS OF INFORMATION, PROGRAMS, OR OTHER DATA) THAT RESULT FROM ACCESS TO, USE OF, OR INABILITY TO USE THE SOLUTIONS, OR DUE TO ANY BREACH OF SECURITY ASSOCIATED WITH THE TRANSMISSION OF INFORMATION THROUGH THE INTERNET, EVEN IF WE WERE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Privacy Policy

Thank you for choosing Ascentis! Ascentis Corporation, and its subsidiaries and affiliates, including, but not limited to NOVAtime Technology, Inc., (collectively “ASC,” “we,” “us,” and “our”) is a leading provider of easy-to-use human capital management and workforce management products and services.

At Ascentis, privacy and transparency around data collection and use are top priorities. This “Privacy Policy” explains how we collect, store, and process your personal information sent to us by you, your employer, or your client, which identifies or could be used to identify you, as further described, below (collectively, “PII” or “Personal Information”).

Policy Scope

This Privacy Policy applies to your access and use of our commercially available versions of our workforce management and human capital management Software-as-a-Service (“SaaS”) solutions, the services related thereto, our publicly available websites (such as, www.ascentis.com and www.novatime.com), and/or the equipment (including, but not limited to, timeclocks, badges, beacons, and beacon readers) rented or sold by us or our partners (collectively, “Solutions”).

We follow this Privacy Policy in conjunction with the applicable laws in the places where we operate. In some cases, we may provide additional terms and conditions which apply to specific Products or Services, or to information we collect from your visit to our publicly available websites. In cases where those terms and conditions conflict with this Privacy Policy, those terms and conditions will control.

Finally, we also process PII sent by or on behalf of your employer (our client) as a result of your employer’s (our client’s) purchase of or subscription to our Solutions. If not otherwise stated in this Privacy Policy or other terms and conditions, we process such PII on behalf of our clients (and their affiliates). We are not responsible for and have no control over the privacy and data security practices of our clients, which may differ from those explained in our Privacy Policy. If your PII has been sent to us by or on behalf of one of our clients, and you wish to exercise any rights you may have under applicable data protection laws, please inquire with them directly.

Types of Personal Information You or Your Employer May Send Us

During the course of your use of our Solutions, we may collect, store, and process, the following types of PII:

- *Identity Information* – first name, last name, picture, social security number, user ID/Employee ID and password for accessing our Solutions.

- *Contact Information* – physical address, email address, telephone number, work location, and department and job data.
- *Employment Information* – employee status, hire date.
- *Application Information* – information submitted with your application for employment, including, but not limited to, information contained in any résumé, curriculum vitae, or cover letters.
- *Bank Data* – if you choose to utilize direct deposit you will be asked to supply bank account data, including, but not limited to, account and routing numbers.
- *Biometric Data* – if you utilize the biometric or finger scanning device on our timeclocks, we may collect data that is based off of your biometric feature (such as your fingerprint, handprint, or face).
- *IP Address or Device Identifier* – We collect your IP address or, if you connect through a mobile device, your mobile device identifier, which identifies the computer, mobile device, or service provider that you use to access our Solutions.
- *Cookies* – Cookies are small text files that can be used by websites to make a user's experience more efficient. Our Solutions use different types of cookies to, among other things, store information regarding your preferences and analyze your use of our Solutions.
- *Web beacons and other technologies* – Our Solutions may use other tracking tools, including web beacons, which are small electronic images embedded in web content and email messages that are not ordinarily visible to users.
- *Usage Information* – We collect details about your use of our Solutions, including log-in information, pages and files viewed, website and webpage interactions (including searches and other actions you take), and date and time stamps associated with your usage.

How we use and disclose your Personal Information

We will strive to use and disclose your PII only as necessary to provide or promote our Solutions to you or our Client, respond to your or our Client's reasonable requests, to improve our Solutions or as permitted by law. The ways in which we may use and share your PII include:

- *Providing our Solutions, including operating our publicly available websites.* We process PII to provide the functionality available in our products, perform our services, or otherwise comply with our contractual obligations in our contract with you or your employer (our client). If we have not entered into a contract with you or your employer (our client), we base the processing on our legitimate interest to operate and administer our websites and provide you with the content you request.
- *Promoting the security of our Solutions.* We process your PII to track use of our Solutions, verify accounts and activity, and investigate suspicious activity.

- *Responding to your contact or support requests.* If you fill out a web form or request user support, whether online or by phone, we process your PII to perform our contract with you or your employer (our client) and to the extent necessary to fulfill your requests or communicate with you.
- *Managing user registrations.* If you register yourself as a user of our Solutions, we use your PII to manage your registration and your account.
- *Managing event registrations, attendance, contests, or promotions.* We process your PII to plan and host events, webinars, contests, and promotions that you have registered for or expressed interest in, including to send communications to you. Some contests and promotions may have additional applicable rules which contain information on how we use your PII.
- *Developing and improving our Solutions.* We process PII to analyze and track usage of our Solutions to the extent it is necessary to develop and provide relevant content and service offerings. We may also process PII to analyze the overall user experience to the extent it is necessary to develop and improve our Solutions.
- *Identifying client opportunities.* We may process your PII to assess new potential client opportunities to the extent processing your PII is necessary to ensure we are meeting the demands of our clients and their users.
- *Registering office visitors.* We process PII to register visitors to our offices, and to manage non-disclosure agreements, to the extent that it is necessary to protect our offices and our confidential information against unauthorized access.
- *Displaying personalized advertisements and content and sending marketing communications.* We process your PII to advertise to you, provide information about us, and provide other personalized content based upon your usage of our Solutions. We also process your PII to send you marketing information, product recommendations, and other similar communications about ourselves or our partners.
- *Enforcing or complying with legal obligations.* We process your PII when cooperating with government authorities, courts or regulators in accordance with our legal obligations under applicable laws. At times we also use PII to enforce our Terms or Service, Privacy Policy, or contracts with our clients.

We may share your Personal Information with the following types of entities:

- *Service Providers*, such as those who provide system administration and hosting, credit card processing, marketing, research and analytics, or customer support.
- *Affiliates*, to the extent that it is required to provide our Solutions to you or our client.

- *Our Clients* (including their affiliates) who are responsible for your use of the Solutions, and to the extent this is necessary to verify accounts and activity, or enforcing our contracts and policies.
- *Professional Advisors*, including lawyers, bankers, auditors, and insurers, who provide consultancy, banking, legal, insurance, and accounting services, and to the extent we are obliged to share your Personal Information.
- *Third Parties Involved in a Corporate Transaction*, such as to a buyer or other successor prior to or in the event of a merger, acquisition, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets, whether as a going concern or as a part of bankruptcy, liquidation, or similar proceeding, where the information is among the assets being transferred, or for any other purpose we disclose when you provide the information.
- *Regulators or Courts*, as required by law, as necessary to comply with a subpoena or similar investigative demand, court order, request for cooperation from law enforcement or other governmental agency, to exercise our legal rights, to defend against legal claims, or as otherwise required by law.

Security of Your Personal Information

We implement commercially reasonable measures to protect your PII, but no method of storage or transmission is completely secure. You are solely responsible for protecting your password, limiting access to your devices, and signing out of websites. Your failure to protect your password, or otherwise securely access and use our Solutions, may increase the risk that your PII is stolen, altered, or compromised without your consent.

How Long We Keep Your Personal Information

We may retain your PII for as long as necessary to meet the original purpose of collection, or as long as required to fulfill our legal obligations. We determine the appropriate retention period for PII we collect on the basis of the nature and sensitivity of the PII being processed, the potential risk of harm from unauthorized use or disclosure of the PII, and the basis of applicable legal requirements, among other things.

Biometric Data

As described above, if you use the biometric scanning feature on one of our timeclocks (which may include, but is not limited to, scanning your fingerprint, handprint, or face), we may create data using a mathematical algorithm based off of your biometric feature (“Biometric Data”) and store that Biometric Data at a site controlled by your employer or in a cloud environment controlled by us.

We only use the Biometric Data for identity verification, workplace security, and fraud prevention purposes. We only store the Biometric Data for so long as you continue to use the

Solutions, or until your employer asks us to delete the Biometric Data. In no cases is the Biometric Data stored or more than one year after you have stopped using the Solutions.

For more information, please see our [Biometric Data Notice](#).

Your Rights in Relation To Your Personal Information

You may have certain rights, under applicable law, relating to your Personal Information, including:

Right to Know. You may request that we disclose to you the categories of, and specific pieces of PII that we collected about you for the twelve month period preceding your request, including:

- The categories of Personal Information we collected;
- The types of sources we collected such Personal Information from;
- The purpose of collecting the Personal Information; and
- The categories of third parties with access to your Personal Information (if any).

Right to Request Deletion of Your Personal Information. You may request that we delete Personal Information that we have collected or maintain about you, to the extent permitted by law.

Right to Opt-Out of Sale of Personal Information. We do not sell your Personal Information.

Right to Non-Discrimination. We will not discriminate against you for choosing to exercise your rights under the law.

Rectify Your Personal Information. You may request that we correct inaccurate Personal Information, taking into account the purpose of processing the Personal Information.

Right to transfer PII to another Data Controller. We will transfer your PII to another Data Controller, to the extent possible.

Right to restrict the processing of your PII. You may object to our processing of your PII for direct marketing purposes, withdraw your consent for our processing of your PII, or otherwise restrict our processing of your PII, to the extent permitted by law.

Other Rights. You may have other rights with respect to your Personal Information as provided under applicable law. Please contact us if you would like to submit a request to exercise one of these rights.

To submit a request to exercise one of these rights, you may contact us at privacy@ascentis.com. Please include the following information in your request: Name, address, details of the specific right you wish to exercise. If you are an authorized agent wishing

to exercise rights on behalf of someone else, please provide us with a copy of their written authorization designating you as their agent.

We will use commercially reasonable efforts to respond to your requests promptly. We will not begin responding to your request until we have verified your identity.

To the extent that your PII was sent to us by your employer (our client), we may not be responsible for and have no control over how to respond to your requests. As a result, if your PII has been sent to us by or on behalf of our client, and you wish to exercise any rights you may have under applicable data protection laws, please inquire with them directly. Because we may only access a client's data upon their instructions, if you do make your request to us directly, please provide us the name of your employer (our client) who submitted your PII to us. We will refer your request to that client and support them as needed.

Third-Party Links

The Solutions may contain links to other companies. If you choose to click on the links and leave our Solutions. Please note that this Privacy Policy no longer applies to the third party websites and we are not responsible for the privacy practices or content of such websites.

Children's Privacy

Our Solutions are intended for adults and are not intended for use by children under the age of 13 years. Accordingly, we do not knowingly collect personal information from children under age 13. If you are a parent or guardian and believe your child has provided us with Personal Information without your consent, please contact us so we can take steps to delete their Personal Information.

Shine to Light

If you are a California resident, California Civil Code 1798.83 permits you to request information regarding the disclosure of your personal information by certain employees of ASC to third parties for the third parties' direct marketing purposes. To make such a request, please send an email to Privacy@Ascentis.com.

Do Not Track

Do Not Track Mechanisms. Because of the changing state of technology and indecision within the industry regarding the meaning of Do Not Track requests, we currently do not make any guarantee that we will honor Do Not Track requests.

Updates to this Privacy Policy

Ascentis reserves the right to amend this Privacy Policy at any time, for any reason, without notice to you, other than the posting of the amended Privacy Policy on the website it is linked to. Changes to this Privacy Policy are effective when they are posted on this page. When we change the policy in a material manner we will let you know by updating the "Effective Date" at

the top of this page. The policies and practices described herein replace all previous notices or statements regarding this subject matter or content of this Privacy Policy.

Contacting Us

If you have any questions or comments about this Privacy Policy please contact Privacy@Ascentis.com or call 800-229-2713 option #5. You may also mail to 11995 Singletree Lane, Suite 400, Eden Prairie, MN 55344.