Anytime AI Data Privacy and Security

Privacy Policy

Last Updated: September 25, 2024 |

Our Privacy Policy articulates the procedures and principles that Anytime AI, Inc., a Delaware corporation ("the Company", or "Anytime AI") and its Affiliates adhere to in the collection, storage, use, disclosure, and processing of information in the course of its business. This includes services provided by the Company's computer software programs through the Company's websites, or by websites that link to this notice (such as Anytime AI™), or the Anytime AI™ internet platform, or to the Company's marketing and sales activities (collectively, the Company's "**Services**"). Within this framework, "**Personal Information**" is defined as any data related to an identified or identifiable individual, covering names, addresses, email addresses, and telephone numbers, among others. "**Sensitive Personal Information**" is a category of Personal Information necessitating enhanced protection due to its nature. This includes data related to ethnic origin, race, marital status, political affiliations, ideological views, religious beliefs, health status, sexual orientation, genetic and biometric data, national identifiers, and records of administrative or criminal proceedings. Additionally, "**Customer Data**" is data uploaded by customers to the Company's website(s), and/or stored on recognized third-party cloud servers with state of the art encryption, security and privacy standards, in connection with the use of the Company's computer software. Customer Data may include Personal Information and Sensitive Personal Information. Except for disclosure of Customer Data only with the express consent of Customer, the Company's policy is to preserve the confidentiality, integrity, and security of Customer Data by encryption so that the Company's computer software processes all such Data without any independent Company access to such Data. For Personal Information and Sensitive Personal Information not embedded in Customer Data, the Company utilizes security and privacy safeguards based on current industry standards. As used herein, the term "Affiliates" has the same meaning as the definition of "Affiliates" set forth in Section 3.1.3 below.

The operation of the Company's licensed computer software program(s) requires interface with third-party subprocessors such as payment processors (i.e., Stripe) and service providers such as Cloud services for storage (i.e. AWS), and/or AI services (i.e., OpenAI), for certain functionalities. The foregoing service providers operate under their own distinct security and privacy policies which comply with industry standards and are beyond the Company's control and jurisdiction. The Company's commitment to data protection is aimed at maintaining the

highest practices and procedures on its own system, as outlined in this document, and arranging for data to be encrypted and housed on recognized Cloud services and/or processed by third-party service providers as described above. The Company encourages users to refer directly to the policies of Cloud services and other third-party service providers for a comprehensive understanding of their security, management and safeguard of customer data (See, e,g, AWS Privacy Notice, OpenAI Privacy Policy).

1. PERSONAL INFORMATION THE COMPANY COLLECTS.

1.1. The Company collects information that alone or in combination with other information in the Company's possession could be deemed in whole or in part to include one or more of the categories of information set forth below. If you choose not to provide such information, the Company may not be able to provide the Company's Services to you or respond to your other requests.

1.1.1. Personal Information You Provide: The Company may collect Personal Information if you create an account to use the Company's Services or communicate with us. The Company does not intentionally collect any Sensitive Personal Information. The Company requests that you refrain from providing Sensitive Personal Information to us.

1.1.2. Communication Information: If you communicate with the Company, it may collect your name, contact information, and the contents of any messages you send.

1.1.3. Payment information: When you purchase or subscribe to the Company's Services, the Company may collect your billing information, such as your credit card number, expiration date, and billing address, or use a third-party payment processor to process your payments.

1.1.4. Personal Information The Company collects through the Company's Social Media Pages: the Company has postings on social media sites like YouTube and LinkedIn ("**Social Media Pages**"). When you interact with the Company's Social Media Pages, the Company will collect Personal Information that you elect to provide to us, such as your contact details. In addition, the companies

that host the Company's Social Media Pages may provide it with aggregate information and analytics regarding the use of the Company's Social Media Pages.

1.1.5. Personal Information. The Company Receives Automatically From Your Use of Company Services: When you visit, use, and interact with the Company's Services, it may receive certain information about your visit, use, or interactions ("**Technical Information**"), including the following:

1.1.5.1. *Log data*: Information that your browser automatically sends whenever you visit the Site ("**Log Data**"). The Log Data the Company will collect includes:

1.1.5.1.1. Browser Type and Settings: Information about the browser you use, including language settings and browser version, which aids it in optimizing the Company's Site for different browser types.

1.1.5.1.2. Date and Time of Your Request: The specific time and date when you access the Company's Site, used for traffic analysis and to understand peak usage times.

1.1.5.1.3. Specific interactions on the Site ("User Interactions"): We track particular interactions on the Site to enhance user experience, improve the Company's content and optimize use of the Company's site. These interactions include:

1.1.5.1.3.1. Clicks: Records the events when a user clicks on links, buttons, images, or other interactive elements on a webpage.

1.1.5.1.3.2. Form Inputs: Records any information you enter into forms (e.g., registration form) on the Company's Site. The Company does not collect

Sensitive Personal Information unless explicitly provided by you.

1.1.5.1.3.3. Visit Duration: Measures the time spent on each page to gauge engagement levels with the Company's content.

1.1.5.1.3.4. Navigation Sequence: Tracks the order of pages you visit.

1.1.5.2. *Usage Data:* The Company collects only the essential information required for the functionality and security of the Company's Services, such as aggregate usage statistics, general performance metrics, and system health data. We do not have operational access to any customer documents or AI queries, or Anytime AI software responses to customers, nor do we store or access any such documents, queries or responses on the Company computer system.

1.1.5.3. *Device information*: The device information the Company collects includes the name of the device, operating system, and browser you are using. Information collected may depend on the type of device you use and its settings.

1.1.5.4. *Cookies*: A cookie is a small string of information that websites you visit transfer to your computer for identification purposes. Cookies are stored on the user's device; the Company's servers do not retain any cookie data. the Company may request cookie-related information from users to facilitate the operation of the Company's product. These cookies are utilized to monitor in real time your engagement with the Company's website in a non-intrusive way, primarily to recall your preferences and assist in navigating between pages efficiently. Cookies are also used for such activities as remembering your access credentials for the Company's Services. In addition to the cookies

used by Anytime AI and the Company's service providers, some cookies are placed by third parties such as Google (for analytics, described below). These third party cookies are not under the Company's control so you should check the website of the third party service providers for more information regarding these cookies. You block cookies by activating the setting on your browser that allows you to refuse the setting of all or some cookies. However, if you use your browser settings to block all cookies (including strictly necessary cookies) you may not be able to access all or parts of the Company's site. By using the Company's Services you agree to the use of cookies for the following purposes:

- *Operational Cookies*: these are essential in order to enable you to move around the website and use its features, such as accessing secure areas of the website, authenticate you and prevent fraudulent use.
- *Functional Cookies*: they remember the operational choices you make, such as language options or the region you are in. These cookies help to make your visit more personal and are deleted automatically when you close your browser or the session expires.

You can turn off all cookies, in case you prefer not to receive them. You can also have your computer warn you whenever cookies are being used. For both options you have to adjust your browser settings (such as Chrome, Safari, Firefox, Edge, or other browser). There are also software products available that can manage cookies for you. Please be aware, however, that when you choose to reject cookies you may limit the features and functionality of the Company's Services.

1.1.6. Customer support information: When you contact the Company for customer support, feedback, or inquiries, the Company may collect your name, email

address, phone number, and any other information you provide it or that the Company requests from you to assist you or resolve your issue ("**Support Information**").

1.2. The following disclosures are intended to provide additional information about (1) the categories of Personal Information the Company collects (as defined above), (2) the source of the Personal Information, (3) how the Company uses each category of Personal Information, and (4) how the Company discloses Personal Information. These disclosures do not limit the Company's ability to use or disclose information as described above.

Category of Personal Information	**Sources of Personal Information**	**Use of Personal Information**	**Disclosure of Personal Information**
Social Information	Your interactions with the Company's Social Media Pages.	Perform analytics and communicate with you.	Our Affiliates.
Payment Information	Direct collection from you.	Process your payment (including through third-party payment processors).	Our Affiliates and third-party payment processors.
Communication Information	Direct communication from you.	Providing the Company's Services and responding to you.	Our Affiliates and service providers.
Technical Information	Your interaction with the Company's Services.	Analytics, moderation, and prevention of fraud and malicious activity.	Our Affiliates and analytics providers.
Support Information	Direct collection from you in the course of providing support.	Providing support, improving the Services, and responding to you.	Our Affiliates.

2. HOW WE USE PERSONAL INFORMATION.

2.1. We do not sell your Personal Information.

2.2. We may use Personal Information for the following purposes:

2.2.1. To send you Software and administrative information. The Company may use your Personal Information to send you information related to the Software and/or information about changes to the Company's terms, conditions, and policies.

2.2.2. To provide, administer, maintain, improve and/or analyze the Services;

2.2.3. To provide you with support services; the Company may use your Personal Information to provide you with requested information or technical support, facilitate resolution of your issue, or to diagnose problems with the Software.

2.2.4. To fulfill and manage your orders. the Company may use your Personal Information to fulfill and manage your orders, registrations, and payments made through the Company's Websites.

2.2.5. To communicate with you including by discussing with you options to use the Anytime AI™ Platform;

2.2.6. To develop new features and services;

2.2.7. To prevent fraud, criminal activity, or misuses of the Company's services, and to ensure the security of the Company's IT systems, architecture, and networks;

2.2.8. To comply with legal obligations and legal process and to protect the Company's rights, privacy, safety, or property, and/or that of Affiliates, you, or other third parties.

3. DISCLOSURE OF PERSONAL INFORMATION.

3.1. The Company is committed to high standards of data privacy and have specific policies in place regarding the handling and disclosure of Personal Information. The Company's operational model ensures that Personal Information is not disclosed to vendors and service providers including cloud service providers, and any information stored on cloud service providers is in encrypted format. The Company's system architecture ensures that cloud service providers are engaged solely for data storage or processing purposes. Robust encryption safeguards are in place, ensuring that these providers do not have access to, nor the ability to

read or interpret, any Personal Information. This approach solidifies the Company's commitment to maintaining the confidentiality and integrity of Customer Data. However, in certain circumstances the Company may share your Personal Information with third parties with or without further notice to you, depending on the context and/or unless required by the law, including without limitation in the situations below:

3.1.1. Business Transfers: If the Company is involved in major business transactions such as reorganization, bankruptcy, receivership, or transition of service to another provider (collectively a "**Transaction**"), your Personal Information and other information may be shared in the due diligence process under non-disclosure agreements with counterparties and others assisting with the Transaction and transferred to a successor or Affiliate as part of that Transaction along with other assets.

3.1.2. Legal Requirements: If required to do so by law or in the good faith belief that such action is necessary to (i) comply with a legal obligation, including to meet national security or law enforcement requirements, (ii) protect and defend the Company's rights or property, (iii) prevent fraud, (iv) act in urgent circumstances to protect the personal safety of users of the Services, or the public, or (v) protect against legal liability.

3.1.3. Affiliates: The Company may share Personal Information with the Company's "**Affiliates**," meaning an entity that controls, is controlled by, or is under common control with Anytime AI, Inc., a Delaware corporation. the Company's Affiliates may use the Personal Information the Company shares in a manner consistent with this Privacy Policy.

3.1.4. Other Users: Actions you take that are designed to be visible within the Company's services, such as posting comments or reviews, may be seen by other users of the Company's services.

3.2. Marketing and advertising. From time to time the Company may contact you with relevant information about the Company's services. Most messages will be sent

electronically. For some messages, the Company may use personal information the Company collects about you to help it determine the most relevant information to share with you regarding the Company's products and services. If you do not want to receive such messages from us, you can change your marketing preferences at any time by following the unsubscribe link at the bottom of the Company's emails.

3.3. Testimonials. With consent, the Company may display personal testimonials of satisfied customers on the Company's site, along with other endorsements. If you wish to update or delete your testimonial, you can contact the Company at admin@anytime-ai.com.

4. CUSTOMER DATA THAT INCLUDES PERSONAL INFORMATION.

Customer Data that the Company's customers upload to the Company's computer software for purposes of utilizing the functionality of the software, or responses to any Customer queries of the software, or that is otherwise stored in connection with the use of the Company's computer software may include Personal Information or sensitive Personal Information. All such Customer Data used with the Company's computer software is encrypted. Customer Data is encrypted, stored by cloud service providers, and owned by Customer, and the Company does not have any independent right, or means of access to the content of such Data except with your express written consent, as described in Paragraph 5.

5. Utilization of Customer Data

The Company does not use any Customer Data to train the Company's AI models without obtaining explicit, informed, and written consent from the Company's customers. The Company's policy of informed consent helps ensure that these limitations on Company use of Customer Data are aimed at full transparency and clear understanding for the Company and the customer as to the parameters of such use. By engaging with the Company's services, you grant Anytime AI a specific, non-revocable right to manage your Customer Data for strictly operational purposes under the following conditions:

- (a) **Service Maintenance and Enhancement:** the Company uses non-encrypted Customer Data generally to maintain and improve the functionality and efficiency of the Company's services. This includes routine operations necessary for service delivery and enhancements based on user feedback.
- (b) **Development of New Features:** The Company may develop new features using aggregated or anonymized data, which ensures that individual data points cannot be traced back to you or any other individual, preserving your privacy.
- (c) **Additional Authorized Uses:** The Company may use Customer Data for other purposes directly authorized by you through specific consent mechanisms.

The Company's access to and use of Customer Data is strictly limited to the purposes for which you have given consent. We do not have the right to independently access, view, or modify Customer Data without such consent. The following measures are in place to safeguard your data:

- **Data Security:** The Company employs stringent security measures, including encryption and access controls, to protect the confidentiality and integrity of your data.
- **Privacy Compliance:** All data handling practices comply with relevant data protection laws, ensuring that your rights and data are protected at all times.

6. CUSTOMER DATA OWNERSHIP.

As per the Company's policy, subject to applicable law, the customer retains ownership rights over data used with the software. This includes data a customer inputs into the Company's computer system and data generated by the Company's product in response to a customer's inquiries, all of which is encrypted and stored on cloud service providers with robust security measures. The Company has no access to such data without your express consent. The Company reinforces your autonomy over your data by providing you with tools to download or delete the data at your discretion. The Anytime AI™ software facilitates your use of your data based on its functionality and enables secure storage of that data and/or responses with no direct access to content by the

Company's or any third party. This approach underscores the Company's commitment to respect and maintain the integrity and confidentiality of your data, with you as owner of the information you choose to use with the Company's product.

7. REQUEST FOR ACTION.

7.1. To request access to or deletion of your Customer Data, please contact the Company at admin@anytime-ai.com. The Company reserves the right to limit the Company's role in facilitating any such requests only to the extent required by applicable law.

7.2. In order to protect your Customer Data from unauthorized access or deletion, the Company may require you to verify, to the Company's satisfaction, your identity visually and/or in writing before the Company will process any request to access or delete Customer Data. If we cannot verify your identity (and, where applicable, proof of residency) to the Company's satisfaction, the Company will not provide or delete your Customer Data. The verification process may include the requirement that you submit sworn statements in a form acceptable to the Company as to your identity and requests.

7.3. You may submit a request to access or delete your Customer Data through an authorized agent. Such an agent must present signed and notarized written authority to act on your behalf and must be able to verify your and the agent's identity (and, where applicable, proof of residency and legal authorization) to a notary public's or the Company's satisfaction.

7.4. We will not discriminate against you for making any such request.

8. SECURITY. In addition to encryption, the Company takes reasonable and appropriate additional steps to protect your Customer Data in an effort to prevent loss, misuse, and unauthorized access, disclosure, alteration and destruction. The Company uses appropriate technical and organizational measures to protect your Customer Data, Personal Information and Sensitive Personal Information which may include: physical access controls, intrusion detection, and network monitoring depending on the nature of the information and the scope of processing. Any Company's staff who may have access for any such purpose are required

to keep any information learned in such processes confidential. Of course, the security of your Customer Data also depends on you. Where you have credentials for access to certain parts of the Company's Website or Software, you are responsible to keep such credentials confidential. The Company cannot guarantee the absolute security of data that is electronically stored or transmitted or received by you over the internet, and there is no guarantee that data may not be accessed, disclosed, altered, or destroyed by breach of any of the Company's physical, technical, or managerial safeguards independent of the Company's computer software, computer system and/or internet platform. If the Company learns of a security breach, the Company may notify you or others consistent with applicable data protection law.

9. **DATA RETENTION AND DELETION**. The Company retains your Customer Data for as long as necessary to fulfill the purposes for which the Company collected it, unless a longer retention period is required or permitted by law. The Company may also retain your Customer Data for legitimate business interests, such as to comply with the Company's legal obligations, resolve disputes, and maintain the Company's records. When the Company no longer needs your Customer Data, we will delete it or anonymize it in accordance with the Company's data retention policies and applicable laws, or, if this is not possible (for example, because your Customer Data has been stored in backup archives), then the Company will securely store your Customer Data and isolate it from any further processing, until deletion is possible.

10. **CHILDREN.** The Company's websites and services are not directed to anyone under the age of 16. Anytime AI™ does not knowingly collect Personal Information from anyone under the age of 16. If you have reason to believe that a minor under the age of 16 has provided Personal Information to Anytime AI™ through the Company's Services, please email it at admin@anytime-ai.com and the Company will endeavor to delete that information from the Company's systems.

11. **LINKS TO OTHER WEBSITES; HACKERS.** The Company's Services may contain links to other websites not operated or controlled by Anytime AI, including social media services ("**Third**

Party Sites"). These links are provided to you for convenience purposes only, and you access them at your own risk. The Company cannot guarantee the safety and privacy of Customer Data you provide to any third parties. Any Customer Data collected by third parties is not covered by this Privacy Policy, and the Company is not responsible for the practices and policies of such third parties, including other websites, services or applications. The information that you share with Third Party Sites will be governed by the specific privacy policies and terms of service of the Third Party Sites and not by this Privacy Policy. By providing these links the Company does not imply that the Company endorses or has reviewed these sites. Please contact the Third Party Sites directly for information on their privacy practices and policies. The Company is not responsible for any loss of Customer Data, Personal Information and/or Sensitive Personal Information that is disclosed as a result of your failure to maintain adequate security and protective measures on your computer system, and/or as a result of any hacking activity on your computer system.

12. **United States Users.** For users residing in the United States, all Customer Data is stored on cloud servers located exclusively within the United States. The Company does not geo-replicate or transfer Customer Data of United States users on servers located in any country outside the United States. This practice is aligned with the Company's commitment to comply with local data protection and privacy regulations applicable to United States users.

13. **INTERNATIONAL USERS.** For users located outside the United States, Customer Data may be stored by the Company or its Affiliates on servers of cloud service providers located in the United States or elsewhere in the world. Notwithstanding the locations of server storage for such users, the terms and conditions of this Privacy Policy apply to such Customer Data, along with the potential need to better comply with the data protection and privacy regulations of your country or locations where data is stored.

14. **RETAINING YOUR INFORMATION.** The Company will only retain your Customer Data for as long as necessary to fulfill the purposes the Company collected it for, including for the purposes of the Company's legitimate business interests and satisfying any legal or

reporting requirements. To determine the appropriate retention period for Customer Data, the Company considers the amount of the Customer Data, the potential risk of harm from unauthorized use or disclosure of your Customer Data, the purposes for which we process your Customer Data and the applicable legal requirements. When the Company no longer has a legitimate business need to process your Customer Data, or if the basis on which we were relying to process your Customer Data no longer applies, the Company will either delete or anonymize your Customer Data. If this is not possible (for example, because your Customer Data is stored in back-up archives), the Company will securely store your Customer Data and isolate it from any further processing until deletion is possible.

15. **REFERRAL PROGRAM.** We operate a referral program for the Company's Service; you may choose to provide it with names and email addresses of individuals who you feel would be interested in learning more about the Company's products and services in exchange for rewards. The Company will store the contact details in order to track the success of the Company's referral service. The referred individual may request that their contact details be removed from the Company's database and they may also contact it at any time at admin@anytime-ai.com to make the request. When you provide the Company with names and email addresses of such individuals as set out above, you will obtain the prior consent of those individuals and provide them with the information as to how we handle their Personal Information as described in this privacy policy.

16. **CHANGES TO THE COMPANY'S PRIVACY POLICY.** The Company may update this Privacy Policy from time to time. When the Company does, it will post an updated version on this page, unless another type of notice is required by applicable law or contractual agreement. By continuing to use the Company's service or providing it with Personal Information after we have posted an updated Privacy Policy, or notified you by other means, you consent to the revised Privacy Policy.

17. **HOW TO CONTACT US.** If you have any questions about the Company's Privacy Policy or privacy-related issues, please contact it at admin@anytime-ai.com.

Security

Last Updated: September 25, 2024 |

We take security of data very seriously. We work hard to protect Other Information you provide from loss, misuse, and unauthorized access or disclosure.

1. Compliance

Anytime AI leverages the robust security standards and compliance certifications of the Company's cloud service providers, enabling us to meet global compliance requirements:

- SOC 2 Type II (AWS compliance)
- GDPR (AWS compliance)
- HIPAA (AWS compliance)
- FedRAMP (AWS compliance)
- FIPS 140-2 (AWS compliance)
- NIST 800-171 (AWS compliance)
- ISO 27001 (AWS compliance)
- CSA (AWS compliance)
- CCPA (AWS compliance)
- PCI (Stripe compliance)

We are committed to upholding the highest standards of data protection and are actively working towards achieving the Company's own certifications to further enhance the Company's security posture and ensure comprehensive protection for the Company's clients.

2. Infrastructure Security

1) **Security infrastructure maintained:** The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
2) **Remote access authentication enforced:** The company's production systems can only be remotely accessed by authorized employees possessing a secure authentication method.
3) **Production database authentication enforced:** The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH keys.
4) **Remote access encryption enforced:** The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.

5) **Encryption key access restricted:** The company restricts privileged access to encryption keys to authorized users with a business need.
6) **Production data segmented:** The company prohibits confidential or sensitive customer data, by policy, from being used or stored in non-production systems/environments.
7) **Production application access restricted:** The company restricts privileged access to the application to authorized users with a business need.
8) **Log management utilized:** The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.
9) **Network segmentation implemented:** The company's network is segmented to prevent unauthorized access to Customer Data.
10) **Network system authentication enforced:** The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.
11) **Firewall access restricted:** The company restricts privileged access to the firewall to authorized users with a business need.
12) **Business Continuity/Disaster Recovery:** The Company has formalized Business Continuity and Disaster Recovery procedures in place, bolstered by a robust monitoring system. This system is designed to detect and respond to incidents efficiently, recover services swiftly, and ensure continuous business operations. The Company's BC/DR strategies are rigorously tested at least annually to verify their effectiveness and to make adjustments as necessary. The Company's use of cloud infrastructure significantly enhances the Company's disaster recovery capabilities. We employ virtual private servers that provide a high degree of reliability and uptime, critical for maintaining operational continuity. The Company's file storage solutions are designed to be automatically backed up and replicated across multiple zones, ensuring data durability and availability. Additionally, the Company's strategy includes regular database backups and comprehensive data management practices to safeguard against data loss. These measures are part of a comprehensive strategy to ensure that the Company's infrastructure can effectively handle various failure scenarios and recover with minimal downtime.

3. Organizational Security

1) **Portable media encrypted:** The company encrypts portable and removable media devices when used.
2) **Password policy enforced:** The company requires passwords for in-scope system components to be configured according to the company's policy.
3) **Confidentiality Agreement acknowledged by contractors:** The company requires contractors to sign a confidentiality agreement at the time of engagement.
4) **Production inventory maintained:** The company maintains a formal inventory of production system assets.

5) **Confidentiality Agreement acknowledged by employees:** The company requires employees to sign a confidentiality agreement during onboarding.
6) **Secure coding:** All releases at Anytime AI require a review from the Company's security team to meticulously examine every component for potential security issues.

4. Product Security

1) **Data encryption utilized:** The Company's datastores housing sensitive customer data are encrypted at rest using an industry standard AES-256 encryption algorithm.
2) **Data transmission encrypted:** The Company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks in order to protect the data from man-in-the-middle attacks.
3) **Automatic backups and redundant servers:** To ensure your account data remains accessible at all times, Anytime AI performs regular automatic backups and makes use of geo-redundancy for its infrastructure.
4) **System activity logged:** The Company captures system activity, including user activity, in transaction logs.
5) **Vulnerability and system monitoring procedures established:** The Company's formal policies outline the requirements for system monitoring.
6) Enforce strong passwords and/or regular password resets with Anytime AI's password policy settings.
7) **Authentication:** Anytime AI™ uses the most up-to-date authentication best practices in order to authorize and authenticate users. Passwords stored in the Company's databases use the latest encryption and salting techniques to prevent attackers from gaining information. The Company's authentication system doesn't rely on automated cookie management schemes that often lead users vulnerable to CSRF attacks. Users and IP addresses are anonymously tracked and monitored to ensure accounts are not breached.

5. Internal Security Procedures

1) **Rigorous access control management:**
    a) **Access requests required**: The Company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.
    b) **Production deployment access restricted**: The Company restricts access to migrate changes to production to authorized personnel.
    c) Only Anytime AI managed devices (including personal mobile devices) can access the Company's internal systems and other external systems.

    d) **Access revoked upon termination:** The Company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.
2) **Change management procedures enforced**: The Company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.
3) **Configuration management system established**: The Company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.
4) **Service description communicated**: The Company provides a description of its products and services to internal and external users.
5) **Support system available**: The Company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.
6) **Roles and responsibilities specified**: Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.