Clearify Platform Privacy Policy

The Clearify platform is owned and operated by ClearTrack HR, LLC. This Consent to the Dependent Verification Services Agreement (this "Agreement"), entered upon your acceptance of these terms, by and between ClearTrack HR, LLC, an Alabama limited liability company (hereinafter referred to as "Service Provider"), and You (hereinafter referred to as "You," or "Your"; Service Provider and You may be referred to individually as a "Party" and collectively as the "Parties").

In consideration of the mutual covenants, promises, and agreements contained in this Agreement, and other good and valuable consideration, the receipt and sufficiency of which is acknowledged, the Parties agree as follows:

The Parties agree that Service Provider, using its best efforts and the information provided by You, shall conduct a dependent verification audit of Your claimed dependents ("Audit"), in accordance with the Dependent Verification Services Agreement, by and between Service Provider and Your employer (the "Audited Company"). All information and data collected is used solely for dependent verification purposes. No user data to be shared outside of verification purposes. You agree to provide certain requested information to Service Provider to facilitate dependent verification. You may be required to either fax, mail, email, or upload documents to support the validity of any claimed dependent.

The term of this Agreement shall be the term of the above-described Dependent Verification Services Agreement. However, You may terminate this Agreement at any time by giving written notice to Service Provider. This Agreement may be terminated by the Service Provider at any time.

You hereby make the following acknowledgements: (1) all information provided to Service Provider by You or the Audited Company will be stored on a web-based platform; (2) You have the authority to disclose any information You provide to Service Provider; (3) You have given permission to audit or use the information disclosed by You or the Audited Company for providing dependent verification services; (4) You have consented to the use of any and all data that Service Provider may have collected previously or may collect in the future; and (5) You are solely responsible for the accuracy and timely input of information to Service Provider.

You hereby grant the following authorizations: (1) to audit the information provided by You or the Audited Company; (2) to use the personal information provided for dependent verification services; and (3) to retain the personal information provided by either You or the Audited Company.

By accepting the rights granted by Service Provider, You agree that You will not, without the prior written consent of Service Provider: (a) attempt to decompile, disassemble, or reverse engineer any program of Service Provider ("Program"); (b) attempt to derive source code or underlying ideas, algorithms, architecture, structure, or organization from the Program; or (c) attempt to defeat, avoid, bypass, remove, deactivate, or otherwise circumvent any software protection mechanisms in the Program, including without limitation any such mechanism used to restrict or control the functionality of the Program.

Information provided by You, which is not generally known to the public, is hereinafter referred to as "Confidential Information." Confidential Information shall be used only for providing dependent verification services. Obligations of confidentiality shall not apply to information that: (a) is or becomes available in the public domain through no wrongful act or omission of Service Provider; (b) is already in Service Provider's rightful possession without an obligation of confidentiality prior to disclosure by You; (c) is rightfully disclosed to Service Provider by a third party without an obligation of confidentiality that is known to Service Provider; (d) is independently developed by Service Provider; or (e) is required to be disclosed by law or pursuant to any order of a court of competent jurisdiction or regulatory order properly served on Service Provider.

Upon the termination of this Agreement and Service Provider's receipt of Your written request, all documents provided to Service Provider shall be destroyed within ten (10) days from the completion of the dependent verification audit period. You agree that any Confidential Information provided under this Agreement may be retained despite the destruction of the underlying documents or termination of this Agreement. Notwithstanding any other terms or conditions contained in the Agreement, Service Provider shall have no duty to retain Confidential Information after termination of the Agreement.

Service Provider reserves all of the rights with respect to the services and the Program under all applicable national and international laws and treaties for the protection of its intellectual property rights, including, but not limited to, trade secrets, copyrights, trademarks, and patents.

Except as otherwise expressly permitted in the Agreement, You shall not cause or permit unauthorized reproduction or disclosure of any portion of the services or the Program or the delivery or distribution of any part thereof to any third party, for any purpose, without the prior written permission of Service Provider. This restriction shall continue beyond the termination of the Agreement. In the event You become aware of any unauthorized use, copying, reproduction, or disclosure of the services or the Program, You agree to promptly notify Service Provider in writing.

Service Provider warrants that: (1) the Audit will be performed in substantial accordance with the terms and conditions contained in the Agreement, and (2) the Confidential Information disclosed under this Agreement will be used solely for dependent verification services. THE PRECEDING WARRANTIES IN THIS PARAGRAPH, ARE THE ONLY WARRANTIES RELATED TO THE SERVICES PROVIDED BY SERVICE PROVIDER AND ARE MADE IN LIEU OF ALL OTHER WARRANTIES AND CONDITIONS, EXPRESS OR IMPLIED INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

In no event shall the aggregate liability of the Service Provider, or its affiliates, to You and the Audited Company, for any reason and for all causes of action, exceed the total Fees paid by the Audited Company under the Dependent Verification Services Agreement. Neither Service Provider, or its affiliates, will be liable under any cause of action, for any indirect, special,

incidental, consequential, reliance or punitive damages, including loss of profits or business interruption.

Any and all notices, invoices, or other documents to be sent under this Agreement will be given via email and will be effective on the first business day after being sent. The email address for notice to Service Provider shall be info@cleartrackhr.com. The email address for notice to You shall be the email address used to register for the Audit. You agree that You are responsible for making any modifications to Your email system in the event communications are treated as "spam" or blocked in any manner. Further, You shall keep Your email address for notice up-to-date.

This Agreement will be governed by and construed under the laws of the State of Alabama without regard to any conflict of laws provisions. The Parties hereby consent and waive all objections to the exclusive personal jurisdiction of, and venue in, federal or state court located in Madison County, Alabama for the purposes of all cases and controversies involving this Agreement. Any action, suit, or proceeding arising under or in connection with the Agreement must be commenced within two (2) years after the claim or cause of action arises.

Any proceeding to resolve or litigate any dispute in any forum will be conducted solely on an individual basis. You agree not to seek to have any dispute heard as a class action or in any proceeding in which either party acts or proposes to act in a representative capacity. No proceeding will be combined with another without the prior written consent of all parties to all affected proceedings. You also agree not to participate in claims brought in a private attorney general or representative capacity, or any consolidated claims involving another person's account, if we are a party to the proceeding. YOU ARE GIVING UP YOUR RIGHT TO PARTICIPATE AS A CLASS REPRESENTATIVE OR CLASS MEMBER ON ANY CLASS CLAIM YOU MAY HAVE AGAINST US INCLUDING ANY RIGHT TO CLASS ARBITRATION OR ANY CONSOLIDATION OF INDIVIDUAL ARBITRATIONS.

If any term of the Agreement is held invalid or unenforceable for any reason, the Parties agree that such invalidity will not affect the validity of the remaining provisions of the Agreement, and the Parties further agree to substitute a valid provision that most closely approximates the intent of the invalid provision.

No part of this Agreement shall be considered waived by Service Provider unless expressly done in writing. Any waiver of any breach or provision of this Agreement shall not operate as or be construed to be a waiver of any subsequent breach or violation. Further, except as otherwise provided herein, the Parties agree this Agreement may only be amended in a writing signed by both Parties.

You may not assign (voluntarily, by operation of law, or otherwise) this Agreement (or any rights or obligations contained herein) without the prior written consent of Service Provider, whose consent shall not be unreasonably withheld. Any permitted assignee shall assume all of Your obligations under this Agreement. Any purported assignment or transfer in violation of this section shall be void.

The Agreement is the entire agreement between You and Service Provider relating to the Audit. The Agreement supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to the Audit or any other subject matter covered by the Agreement.

This Agreement shall become effective immediately upon Your acceptance of these terms as acknowledged by marking the box indicating Your acceptance.

RECORD RETENTION AND DESTRUCTION POLICY

1) Purpose

The purpose of this Policy is to ensure that necessary records and documents of are adequately protected and maintained and to ensure that records that are no longer needed by Cleartrack HR or are of no value are discarded at the proper time. This Policy is also for the purpose of aiding employees of Cleartrack HR in understanding their obligations in retaining electronic documents - including e-mail, Web files, text files, sound and movie files, PDF documents, and all other formatted files.

2) Policy

This Policy represents the Cleartrack HR's policy regarding the retention and disposal of records and the retention and disposal of electronic documents.

3) Administration

Attached as Appendix A is a Record Retention Schedule that is approved as the initial maintenance, retention, and disposal schedule for physical records of Cleartrack HR and the retention and disposal of electronic documents. The Policy Administrator (the "Administrator") is the officer in charge of the administration of this Policy and the implementation of processes and procedures to ensure that the Record Retention Schedule is followed. The Administrator is also authorized to make modifications to the Record Retention Schedule from time to time to ensure that it is in compliance with local, state and federal laws and includes the appropriate document and record categories for Cleartrack HR; monitor local, state and federal laws affecting record retention; annually review the record retention and disposal program; and monitor compliance with this Policy.

4) Suspension of Record Disposal in Event of Litigation or Claims

In the event Cleartrack HR is served with any subpoena or request for documents or any employee becomes aware of a governmental investigation or audit concerning Cleartrack HR or the commencement of any litigation against or concerning Cleartrack HR, such employee shall inform the Administrator and any further disposal of documents shall be suspended until shall time as the Administrator, with the advice of counsel, determines otherwise. The Administrator shall take such steps as is necessary to promptly inform all staff and ownership group of any suspension in the further disposal of documents.

5) Applicability

This Policy applies to all physical records generated in the course of Cleartrack HR's operation, including both original documents and reproductions. It also applies to the electronic documents described above.

This Policy was approved by the executive management team of Cleartrack HR

6) Disposal Procedures

All information will be disposed/removed upon the frequencies mentioned in "Appendix A – Record Retention Schedule" Any and all client(s) pertains the right for any and all data, not detrimental to the business, to be disposed/removed. All disposal requests will be presented in writing by client based upon that client's specific service agreement. At that point, the Senior Architect shall be notified of specific client, service, type of disposal, and requested date of disposal. All disposal requests will be presented to the executive management team as soon as request is received.

Senior Architect will delete client's FTP folder and account utilizing SFTP Administrator. Senior Architect will utilize Azure Portal to delete all applicable database information.

Upon completion of disposal, the Senior Architect will notify the executive management team, in writing, of the executed data disposal. Assigned representative from the executive management team will notify client, affected parties, and/or any applicable legal authorities, in writing, of the successful disposal of data.

APPENDIX A - RECORD RETENTION SCHEDULE

The Record Retention Schedule is organized as follows:

SECTION TOPIC

A. Accounting and Finance
B. Contracts
C. Corporate Records
D. Electronic Documents
E. Insurance Records
F. Legal Files and Papers
G. Miscellaneous
H. Payroll Documents
I. Personnel Records

A. ACCOUNTING AND FINANCE

Record Type	Retention Period
Accounts Payable ledgers and schedules	7 years
Accounts Receivable ledgers and schedules	7 years
Financial Statements	Permanent
Bank Statements and Canceled Checks	7 years
Employee Expense Reports	7 years
Credit card records (documents showing customer credit card number)	7 years

1. Credit card record retention and destruction

   A credit card may be assigned to management to be used to pay for the operations of Cleartrack HR products and services, all transactions are monitored and must be approved by management

B. CONTRACTS

Record Type	Retention Period
Contracts and Related Correspondence	7 years after expiration or terminatio
	Permanent

C. CORPORATE RECORDS

Record Type	Retention Period
Licenses and Permits	Permanent

D. ELECTRONIC DOCUMENTS

1. **Electronic Mail**: Not all email needs to be retained, depending on the subject matter..
   - Staff will strive to keep all but an insignificant minority of their e-mail related to business issues.
   - Cleartrack HR will archive e-mail upon employees termination
   - Staff will take care not to send confidential/proprietary Cleartrack HR information to outside sources.

2. **Electronic Documents**:
   - **PDF documents** – The length of time that a PDF file should be retained should be based upon the content of the file and the category under the various sections of this policy. The maximum period that a PDF file should be retained is 6 years. PDF files the employee deems vital to the performance of his or her job should be printed and stored in the employee's workspace.
   - **Text/formatted files** - Staff will conduct annual reviews of all text/formatted files and will delete all those they consider unnecessary or outdated. After five years, all text files will be deleted from the network and the staff's desktop/laptop. Text/formatted files the staff deems vital to the performance of their job should be printed and stored in the staff's workspace.
   - **Clearify submitted verification documents** – All submitted verification documents are stored for a minimum of 7 years to meet HIPPA requirements. Verification documents storage time frame can be adjusted upon client request. Request must be in writing as an amendment to service contract. Aged documentation will be removed unless deemed necessary for the business to retain.

3. Web Page Files: Internet Cookies

Cookies should be cleared by employee on a quarterly basis. Cleartrack HR does not automatically delete electronic files beyond the dates specified in this Policy. It is the responsibility of all staff to adhere to the guidelines specified in this policy.

Backup copy of all electronic files (including email) on Cleartrack HR's servers. This backup is a safeguard to retrieve lost information should documents on the network experience problems. The tbackup copy is considered a safeguard for the record retention system of Cleartrack HR, but is not considered an official repository of Cleartrack HR records.

In certain cases, a document will be maintained in both paper and electronic form. In such cases the official document will be the electronic document.

E. INSURANCE RECORDS

Record Type	Retention Period
Annual Loss Summaries	10 years
Audits and Adjustments	3 years after final adjustment
Certificates Issued to Cleartrack HR	Permanent
Claims Files (including correspondence, medical records, injury documentation, etc.)	Permanent
Group Insurance Plans - Active Employees	Until Plan is amended or terminated
Insurance Policies (including expired policies)	Permanent

F. LEGAL FILES AND PAPERS

Record Type	Retention Period
Legal Memoranda and Opinions	7 years after close of matter
Litigation Files	1 year after expiration of appeals or time for filing appeals
Court Orders	Permanent

G. MISCELLANEOUS

Record Type	Retention Period
Statistical Analysis and Reports	7 years
Policy and Procedures Manuals	Current version with revision history
Annual Reports	Permanent

H. PAYROLL DOCUMENTS

Record Type	Retention Period
Employee Deduction Authorizations	4 years after termination
Payroll Deductions	Termination + 7 years
W-2 and W-4 Forms	Termination + 7 years
Garnishments, Assignments, Attachments	Termination + 7 years
Payroll Registers (gross and net)	7 years

I. PERSONNEL RECORDS

Record Type	Retention Period
Commissions/Bonuses/Incentives/Awards	7 years
Employee Earnings Records	Separation + 7 years
Employee Handbooks	Permanently
Employee Medical Records	Separation + 6 years
Employee Personnel Records	6 years after separation
Employment Contracts – Individual	7 years after separation
Employment Records - Correspondence with Employment Agencies and Advertisements for Job Openings	3 years from date of hiring decision
Employment Records - All Non-Hired Applicants (including all applications and resumes - whether solicited or unsolicited, results of post-offer, pre-employment physicals, results of background investigations, if any, related correspondence)	4 years
Job Descriptions	3 years after superseded
Personnel Count Records	3 years
Forms I-9	3 years after hiring, or 1 year after separation if later

Cleartrack HR Data Classification Policy

POLICY STATEMENT

1. Information Services (IS) Responsibility—All IS employees who come into contact with sensitive information are expected to familiarize themselves with this data classification policy and to consistently use these same ideas in their daily Cleartrack HR business activities. Sensitive information is either Confidential or Restricted information. Although this policy provides overall guidance, to achieve consistent information protection, IS employees are expected to apply and extend these concepts to fit the needs of day-to-day operations. This document provides a conceptual model for IS for classifying information based on its sensitivity, and an overview of the required approaches to protect information based on these same sensitivity classifications.

2. Addresses Major Risks - The IS data classification system, as defined in this document, is based on the concept of need to know. This term means that information is not disclosed to any person who does not have a legitimate and demonstrable business need to receive the information. This concept, when combined with the policies defined in this document, will protect Cleartrack HR information from unauthorized disclosure, use, modification, and deletion.

3. Applicable Information - This data classification policy is applicable to all electronic information for which IS is the custodian.

PROCEDURES

1. Access Control

1.1 Need to Know—Each of the policy requirements set forth in this document are based on the concept of need to know. If an IS employee is unclear how the requirements set forth in this policy should be applied to any particular circumstance, he or she must conservatively apply the need to know concept. That is to say that information must be disclosed only to those people who have a legitimate business need for the information.

1.2 System Access Controls—The proper controls shall be in place to authenticate the identity of users and to validate each user's authorization before allowing the user to access information or services on the system. Data used for authentication shall be protected from unauthorized access. Controls shall be in place to ensure that only personnel with the proper authorization and a need to know are granted access to Cleartrack HR systems and their resources. Remote access shall be controlled through identification and authentication mechanisms.

1.3 Access Granting Decisions—Access to Cleartrack HR sensitive information will be based on job duties and based on business needs. Special needs for other access privileges will be dealt with on a request-by-request basis by the executive management team. The list of individuals with access to Confidential or Restricted data must be reviewed for accuracy by the relevant Data Owner in accordance with a system review schedule approved by the executive management team.

2. Information Classification

2.1 Owners and Production Information—All electronic information managed by IS must have a designated Owner. Production information is information routinely used to accomplish business objectives. Owners are responsible for assigning appropriate sensitivity classifications as defined below. Owners do not legally own the information entrusted to their care. They are instead designated members of the Cleartrack HR management team who act as stewards, and who supervise the ways in which certain types of information are used and protected.

2.2 RESTRICTED—This classification applies to the most sensitive business information that is intended for use strictly within Cleartrack HR. Its unauthorized disclosure could seriously and adversely impact Cleartrack HR, its customers, its business partners, and its suppliers.

2.3 CONFIDENTIAL—This classification applies to less-sensitive business information that is intended for use within Cleartrack HR. Its unauthorized disclosure could adversely impact Cleartrack HR or its customers, suppliers, business partners, or employees.

2.4 PUBLIC—This classification applies to information that has been approved by Cleartrack HR management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be disseminated without potential harm.

2.5 Owners and Access Decisions—Data Owners must make decisions about who will be permitted to gain access to information, and the uses to which this information will be put. IS must take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of electronic information.

3. Object Reuse and Disposal

Storage media containing sensitive (i.e. restricted or confidential) information shall be completely empty before reassigning that medium to a different user or disposing of it when no longer used. Simply deleting the data from the media is not sufficient. A method must be used that completely erases all data. When disposing of media containing data that cannot be completely erased it must be destroyed in a manner approved by the Director of IS Security.

4. Physical Security

4.1 Data Center Access—Access to the data center must be physically restricted in a reasonable and appropriate manner. - Currently not applicable

4.2 Facility Access–All network equipment and servers located in the corporate office and in all facilities must be secured when no Cleartrack HR personnel, or authorized contractors, are present. Physically secured is defined as locked in a location that denies access to unauthorized personnel.

5. Special Considerations for Restricted Information

If Restricted information is going to be stored on a personal computer, portable computer, or any other single-user system, the system must conform to data access control safeguards approved by IS and executive management. When these users are not currently accessing or otherwise actively using the restricted information on such a machine, they must not leave the machine without logging off,

invoking a password protected screen saver, or otherwise restricting access to the restricted information.

Hot corners must also be established on every issued computer.

5.1 Data Encryption Software—Cleartrack HR employees and vendors must not install encryption software to encrypt files or folders without the express written consent of IS Security.

6. Information Transfer

6.1 Transmission Over Networks—If Cleartrack HR Restricted data is to be transmitted over any external communication network, it must be sent only in encrypted form. Such networks include electronic mail systems, the Internet, etc. All such transmissions must use a virtual public network or similar software as approved by the Information Security Team. Detailed breakdown of email protocols can be found in the "Cleartrack HR IT Security Policy"

6.2 Transfer To Another Computer—Before any Restricted information may be transferred from one computer to another, the person making the transfer must ensure that access controls on the destination computer are commensurate with access controls on the originating computer. If comparable security cannot be provided with the destination system's access controls, then the information must not be transferred.

7. Software Security

7.1 Secure Storage of object and source code—Object and source code for system software shall be securely stored when not in use by the developer. Any changes to production applications must follow the change management process.

7.2 Testing—Developers must at least perform unit testing. Final testing must be performed by the Quality Assurance team or assigned team representative/staff.

7.3 Backups—Sensitive data shall be backed up regularly, and the backup media shall be stored in a secure environment. See "Cleartrack HR IT Security Policy" for detailed backup procedures

8. Key Management

8.1 Protection of Keys—Public and private keys shall be protected against unauthorized modification and substitution.

8.2 Procedures—Procedures shall be in place to ensure proper generation, handling, and disposal of keys as well as the destruction of outdated keying material.

8.3 Safeguarding of Keys—Procedures shall be in place to safeguard all cryptographic material, including certificates. IS Security must be given copies of keys for safekeeping.

9. Calculating Classification - The goal of information security is to protect the confidentiality, integrity, and availability of Institutional Data. Data classification reflects the level of impact to Cleartrack HR if confidentiality, integrity, or availability is compromised.

In some situations, the appropriate classification may be more obvious, such as when federal laws require Cleartrack HR to protect certain types of data (e.g., personally identifiable information). If the appropriate classification is not inherently obvious, consider each security objective using the following table as a guide. It is an excerpt from Federal Information Processing Standards ("FIPS") publication 199 published by the National Institute of Standards and Technology, which discusses the categorization of information and information systems.

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

As the total potential impact to Cleartrack HR increases from Low to High, the classification of data should become more restrictive moving from Public to Restricted. If an appropriate classification is still unclear after considering these points, contact the executive management team for assistance.