Section 1 Purpose

To provide guidance to ONESTREAM NETWORKS staff members, employees, consultants, contractors, distributors, temporary workers, suppliers, agents, representatives, partners, affiliates, and all personnel affiliated with such third parties ("Covered Persons") on the management of EU Personal Data (as defined below) processed by or on behalf of ONESTREAM NETWORKS, in accordance with the EU General Data Protection Regulation ("GDPR"). This policy describes how Personal Data must be collected, handled, and stored to meet ONESTREAM NETWORKS's data protection standards, and to comply with GDPR. The purpose of this policy is to ensure fair and transparent processing of Personal Data.

Section 2 Scope

ONESTREAM NETWORKS's policy is to respect and protect Personal Data collected or maintained by or on behalf of ONESTREAM NETWORKS. All Personal Data must be processed in a lawful, fair, and transparent manner and it is ONESTREAM NETWORKS's duty to ensure the security and confidentiality of such Personal Data at all times. This policy covers all Personal Data obtained from ONESTREAM NETWORKS's candidates, employees and former employees, customers and potential customers and third-parties, including information relating to patients of ONESTREAM NETWORKS's customers (e.g., a customer's identification number relating to a patient is Personal Data under GDPR, even if it does not allow ONESTREAM NETWORKS to directly identify said patient).

In accordance with GDPR, this policy outlines the technical measures and organizational procedures under which ONESTREAM NETWORKS safeguards Personal Data from unauthorized use, access, modification, destruction, or disclosure. This policy applies regardless of whether the data is stored electronically, on paper or in other formats, and regardless of the place where such data may be stored.

Section 3 Definitions

"Biometric Data" means Personal Data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

"Consent" means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, agrees to the processing of personal data relating to him or her.

"Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by ONESTREAM NETWORKS.

"Data Concerning Health" means Personal Data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

"DPIA" means a data protection impact assessment.

"Data Subject" means a natural person in the EU who can be identified, directly or indirectly. For purposes of this policy, data subject shall be limited to employees, former employees, customers, customers' patients and potential customers of ONESTREAM NETWORKS.

"Genetic data" means Personal Data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that person and which result from an analysis of a biological sample from the person in question.

"Personal Data" means any information relating to an identified or identifiable EU natural person. An identifiable person is someone who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data (e.g. GPS coordinates), online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person including name, address, online identifiers including an IP address, email address, etc. When in doubt, treat the information as Personal Data.

"Processing" means anything that is done to, or with, Personal Data including collecting, recording, using, disclosing by transmission, dissemination or otherwise making available, storing or deleting the Personal Data.

"Special Category Personal Data" means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

"Third Party" means any natural or legal person (i) that is not a subsidiary, employee, or director of ONESTREAM NETWORKS or any vendor, provider or processor of ONESTREAM NETWORKS and (ii) that is not authorized to process Personal Data on behalf of and under the instructions of ONESTREAM NETWORKS, either by law or by contract.

Section 4 Responsibilities

- HR is responsible for protecting Personal Data of ONESTREAM NETWORKS's candidates, employees and former employees. HR and the Legal Department are responsible for evaluating any third-party vendor, provider or processor ONESTREAM NETWORKS is considering using to store or process Personal Data. For instance, recruitment agencies, payroll services and other benefits providers.
- The IT Department is responsible for ensuring all systems, services and equipment used for storing data meet acceptable security standards. Performing regular checks and scans to ensure security hardware and software is functioning properly. Evaluating any third-party vendor, provider or processor ONESTREAM NETWORKS is considering using to store or process data. For instance, cloud computing services.
- The Legal Department is responsible for approving any data protection statements attached to documentation and communications provided to candidates, employees and former employees as well as documentation and communications sent to Customers of ONESTREAM NETWORKS, such as emails and letters or information notices displayed on ONESTREAM NETWORKS's websites.

- The Legal Department is responsible for addressing any data protection queries from individuals, journalists, or media outlets like newspapers.
- All Covered Persons are responsible for taking steps designed to protect Personal Data and shall adhere to the procedures defined in this policy and, as the case may be, in the contract entered with ONESTREAM NETWORKS.
- Anyone involved in the processing of Personal Data, including the Covered Person who has access to Personal Data as part of their functions at ONESTREAM NETWORKS or that obtained the Personal Data pursuant to a business relationship with ONESTREAM NETWORKS, is accountable for taking reasonable and appropriate steps designed to protect the Personal Data, including but not limited to compliance with applicable laws, regulations, and ONESTREAM NETWORKS policies and procedures.
- Each business unit and their respective departments are responsible for working with the Legal Department, and IT Department to implement appropriate compliance controls specific to their operations (including but not limited to business practices, other guidance, and training of Covered Persons), in particular the vetting of any potential or current vendor, provider or processor to which Personal Data may be transferred or disclosed, as part of their business relationship with ONESTREAM NETWORKS. Covered Persons are required to follow the applicable business practices and other guidance, and to take the training required by their business units and/or departments.

Section 5 Lawful Basis

All Personal Data should be processed by lawful and fair means, in a transparent fashion. It is important to ensure that at all points where Personal Data is collected, individuals are provided with appropriate notice and information as to the use of their Personal Data, including whether automated processing is used. Covered Persons should limit Personal Data processing to the minimum amount necessary to accomplish the purpose for which such Personal Data is collected, pursuant to ONESTREAM NETWORKS's policies and procedures.

The processing of Personal Data will only be lawful if it satisfies at least one of the following conditions:

- ONESTREAM NETWORKS has consent from the individual. Covered Persons are responsible for keeping a record of when and how they received consent from the individual.
- Necessary for the performance of a contract with the data subject or to take steps preparatory to such a contract
- Necessary for compliance with a legal obligation bearing on ONESTREAM NETWORKS. The legal obligation must be an obligation of Member State or EU law to which ONESTREAM NETWORKS is subject.
- Necessary to protect the vital interests of a data subject or another person where the data subject is incapable of giving consent. (e.g. medical emergency)
- Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in ONESTREAM NETWORKS. There must be a clear basis under Member State or EU law.
- Necessary for the purposes of legitimate interests: the processing is necessary to achieve the legitimate interests of ONESTREAM NETWORKS or a third-party, provided that such legitimate interest is balanced against the individual's interests, rights and freedoms and such do not prevail.
- Covered Persons are responsible for documenting the lawful basis for collecting Personal Data.

Section 6 Special Categories of Personal Data

As a general policy, Covered Persons should not collect, use, disclose, store, or otherwise process any Special Category Personal Data about ONESTREAM NETWORKS's customers or potential customers. However, in certain circumstances, Covered Persons may have incidental or inadvertent contact with Personal Data of a patient of ONESTREAM NETWORKS's customers or potential customers in the course of their activities with ONESTREAM NETWORKS. In order to lawfully process Special Category Personal Data, Covered Persons must work with the Legal Department to identify both a lawful basis and one of the following conditions:

- ONESTREAM NETWORKS has explicit consent to the processing of the Personal Data;
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of ONESTREAM NETWORKS or of the data subject in the field of employment and social security and social protection law in so far as it is authorized by GDPR (e.g. trade union membership or health condition for health insurance purposes);
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent (e.g. medical emergency);
- processing relates to personal data which are manifestly made public by the data subject (e.g. in the context of background checks);
- processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional;
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Section 8 Use Limitation

- Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes, save the case where prior information relating to this further purpose is provided and data subjects' consent thereto is collected, as the case may be.
- Personal Data collection should be relevant to the purposes for which the Personal Data is to be used, and to the extent necessary for those purposes, should be accurate, complete and kept up-to-date, where applicable.
- Personal Data should not be disclosed, made available or otherwise used for purposes other than those specified under a contract with a ONESTREAM NETWORKS customer, except upon the written instructions of the customer, or by the authority of law.
- If Personal Data is disclosed in any manner permitted by applicable law, any Third-Party that receives the Personal Data (including agents and subcontractors) must agree in writing to the same restrictions and conditions that apply under the applicable ONESTREAM NETWORKS customer contract.
- Personal Data should only be collected when directly relevant and necessary to accomplish the specified purpose(s) for which it has first been collected by or on behalf of ONESTREAM NETWORKS.
- Personal Data should only be retained for as long as is necessary to fulfill the specified purpose(s) for which it has first been collected by or on behalf of ONESTREAM NETWORKS and in accordance with ONESTREAM NETWORKS's retention policies.
- Covered Persons should notify a designated supervisor of any written request by an individual for access to recorded Personal Data or Personal Data about that or another individual; requests from individuals outside of ONESTREAM NETWORKS should always be reported to the Legal Department immediately.

Section 9 Security Safeguards

All Covered Persons shall maintain appropriate administrative, technical, and physical safeguards designed to help ensure the security and confidentiality of Personal Data, taking into account the risks and the nature of the Personal Data to be protected, in order to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed pursuant to any policy of ONESTREAM NETWORKS. Examples include but are not limited to the following:

- Limiting disclosure of Personal Data to those who need access for limited authorized business purposes.

- Immediately inform a designated supervisor, the Legal Department, and IT of any actual or suspected system breaches, vulnerabilities or risks.
- Do not input into ONESTREAM NETWORKS systems (including ONESTREAM NETWORKS apps) any Sensitive Special Category Personal Data unless authorized by the Legal Department in writing.
- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Make sure paper and printouts are not left where unauthorized people could see them, and all materials and copies should be collected in a timely manner.
- Documents should be shredded and disposed of securely when no longer required.
- Use passwords that are changed regularly and never shared between Covered Persons.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- The IT Department will make sure servers containing personal data are in a secure location, away from general office space.
- ONESTREAM NETWORKS's data should be backed up frequently. Those backups should be tested regularly, in line with ONESTREAM NETWORKS's standard backup procedures.
- Personal Data should never be saved directly to ONESTREAM NETWORKS's laptops or other mobile devices like tablets or smart phones. Covered Persons shall be prohibited from using private personal devices to access and or otherwise use or store Personal Data.
- IT will ensure that Data is protected from unauthorized access, accidental deletion and malicious hacking attempts by installing approved security software and firewalls.
- New Employee Training
- Visitors to area of Personal Data collection and/or filing should be escorted at all times when on premises.
- Personal Data material to be discarded should be cross-cut shredded and electronic media destroyed pursuant to IT department instructions such that the Personal Data cannot be read or reconstructed.
- When possible, Personal Data should be de-identified, pseudonymized, redacted or encyrpted.

Security Breaches

All Covered Persons, business units and departments shall work with the Legal Department and IT to comply with ONESTREAM NETWORKS's Data Breach Policy

Reporting Inappropriate Use or Disclosure of Personal Data

If a Covered Person feels that an individual's privacy or confidentiality has been violated or that Personal Data has been accessed, used, acquired or disclosed in an unauthorized manner or in a manner otherwise contrary to this policy, he or she should immediately report the incident to the Legal Department.

Section 10 Data Subject Request

If you receive a request from a Data Subject, please report it to the Legal Department immediately.
It is ONESTREAM NETWORKS duty to respond to a request by a Data Subject promptly and in any event within one month of receipt of the request.

Section 11 Third Party Supplier

If a third-party vendor, provider or supplier processes Personal Data on behalf of ONESTREAM NETWORKS, ONESTREAM NETWORKS must have in place a written contract stating that the processor will only act under the instructions of ONESTREAMNETWORKS and that they comply with data security obligations equivalent to those imposed on ONESTREAM NETWORKS. All business units and departments shall work with IT and the Legal Department to:

- Take reasonable steps to select and retain approved suppliers that can maintain appropriate security measures to protect Personal Data in a manner consistent with this policy and any applicable laws.
- Require third-party suppliers by contract to implement and maintain appropriate technical and organizational security measures for Personal Data and to protect Personal Data from unauthorized access, destruction, use, modification, or disclosure;
- Identify third-party suppliers to or from which ONESTREAM NETWORKS transmits Special Category Personal Data or that store such Personal Data on laptops and mobile devices so that the IT Department can provide mechanisms and measures for the encryption of such transmissions, laptops, and mobile devices, as appropriate;
- Train Covered Persons to encrypt Special Category Personal Data before sending it to a third-party supplier;
- Require third-party supplier to report information security incidents and breaches to ONESTREAM NETWORKS without delay following discovery of such breach (ideally between 24 / 48 hours) and provide evidence relating to such breach context and extent; and
- Monitor supplier for compliance with their data protection obligations and, in case of any doubt, mandate an audit of such supplier data protection practices, in compliance with the agreement entered with ONESTREAM NETWORKS.