# DATA USE AND PROCESSING POLICY

The following Data Use and Processing Policy describing the data use and processing requirements between National Marrow Donor Program ("NMDP") and Center, each a "Party" and collectively, the "Parties") reflects the arrangements that they have agreed to put in place pertaining to the Parties' data privacy and security obligations in performing their respective responsibilities in facilitating the sharing of Personal information between the Parties.

As such, the Parties agree to share Personal Information with each other and agree to use Personal Information according to the terms set out herein.

**1. Definitions.**

(a) "**Authorized Persons**" –, and who are bound in writing by confidentiality obligations sufficient to protect Personal Information in accordance with the terms and conditions of the Agreement.

(b) **"Personal Information"** means information provided by a Party hereto (the "Disclosing Party") to the other Party hereto (the "Receiving Party") or at the direction of the Disclosing Party, or to which access was provided to Receiving Party by or at the direction of the Disclosing Party, in the course of Disclosing Party's performance under the Agreement that: (i) identifies or can be used to identify an individual (including, without limitation, names, signatures, addresses, telephone numbers, e-mail addresses, medical records and unique identifiers); or (ii) can be used to authenticate an individual (including, without limitation, employee identification numbers, government-issued identification numbers, passwords or PINs, financial account numbers, credit report information, biometric or health data, answers to security questions and other personal identifiers).

(c) **"Security Breach"** means [(i)] any act or omission that materially compromises either the security, confidentiality or integrity of Confidential Information or the physical, technical, administrative or organizational safeguards put in place by Receiving Party, or any Authorized Persons, that relate to the protection of the security, confidentiality or integrity of Confidential Information, or (ii) receipt of a complaint in relation to the privacy practices of Receiving Party, or any Authorized Persons, or a breach or alleged breach of this Agreement relating to such privacy practices.

(d) **"Confidential Information"** All information, materials, discussions and proceedings which Receiving Party will be party to under the Agreement (including but not limited to proprietary and trade secret information, and Personal Information are, and shall be held and maintained by Receiving Party as, confidential ("Confidential information").

(e) **"Disclosing Party"** means the Party which discloses or makes available, directly or indirectly, its Personal Information or Confidential Information to the other Party.

(f) **"Receiving Party"** means the Party which receives or obtains, directly or indirectly, Personal Information or Confidential Information of the other Party.

**2. Privacy Requirements**

(a) Receiving Party represents and warrants that its collection, access, use, storage, disposal and disclosure of Personal Information does and will comply with all applicable federal, state, and international privacy and data protection laws, as well as all other applicable regulations and directives.

(b) Receiving Party must only process Personal Information on the documented instructions of the Disclosing Party and within the means outlined in the Agreement or Exhibits. Processing outside of this purpose or means requires prior approval by Disclosing Party and a formal adjustment to the Agreement.

(c) The Parties cooperatively will maintain an Agreement which specifies the data subject matter, duration of processing, nature and purpose of processing, types of Personal Information, and categories of data subjects.

(d) At the request of Disclosing Party, Receiving Party shall provide a list of all of the entities and locations at which Personal Information is stored (including where Personal Information is stored by any Subcontractors).

(e) Receiving Party must not, without Disclosing Party's prior written consent, make an international transfer of Personal Information.

(f) Receiving Party shall not, without Disclosing Party's prior written consent, subcontract any of its rights and obligations under the Agreement between the Parties or make any material variation to a subcontract arrangement. Consent shall not be required to subcontract to an affiliate of Receiving Party or to a subcontractor approved by the Disclosing Party. For the avoidance of doubt, the appointment of any processor in respect of Personal Information shall constitute subcontracting for the purposes of the Agreement.

(g) Disclosing Party's consent to any subcontracting will not relieve Receiving Party of its obligations to NMDP under the Agreement and Receiving Party shall be fully responsible for the acts or omissions of its subcontractors and personnel.

(h) Receiving Party shall ensure that all subcontractors comply with the Confidential Information security obligations required under the Agreement. Receiving Party's subcontractor agreements shall include written privacy and data safeguarding obligations consistent with the requirements of the Agreement.

(i) Receiving Party must assist the Disclosing Party, as applicable, in fulfilling Disclosing Party's data controller duties. Upon reasonable request by the Disclosing Party, Receiving Party must assist Disclosing Party in (1) keeping Personal Information secure, (2) notifying the appropriate supervisory authority as necessary, (3) advising data subjects when there has been a Security Breach, (4) carrying out data protection impact assessments (DPIA), (5) consulting the supervisory authority when the DPIA indicates there is an unmitigated high risk to the processing, and (6) assist Disclosing Party in fulfilling requests from individuals exercising their rights under data protection legislation.

(j) Receiving Party must obtain a commitment of confidentiality from anyone it allows to process the Personal Information, unless they are already under such a duty by law.

(k) Receiving Party must inform Disclosing Party immediately if given instruction which does not comply with applicable data protection laws.

(l) Receiving Party must designate a Data Protection Officer (DPO) who maintains expert knowledge of data protection laws and practices. The DPO will be responsible for monitoring and enforcing data protection compliance to the terms of the Agreement.

(m) Receiving Party agrees that nothing in the Agreement relieves the Disclosing Party of their own direct responsibilities and liabilities under applicable security and privacy laws.

(n) Receiving Party must not, without Disclosing Party's prior written consent, track or profile Disclosing Party's users, including through the use of persistent cookies or web beacons.

**3. <u>Security Safeguard and Security Breach Requirements</u>.**

(a) Receiving Party shall implement administrative, physical and technical safeguards to protect Confidential Information, as defined in the Agreement, that are no less rigorous than accepted industry practices including the International Organization for Standardization's standards: ISO/IEC 27001:2013 (or any successor) – Information Security Management Systems , and shall ensure that all such safeguards, including the manner in which Confidential Information is collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of the Agreement.

(b) At a minimum, Receiving Party's safeguards for the protection of Confidential Information shall include: (i) limiting access of Confidential Information to Authorized Employees; (ii) securing business facilities, data centers, paper files, servers, back-up systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (iii) implementing network, device application, database and platform security; (iv) securing information transmission, storage and disposal; (v) implementing authentication and access controls within media, applications, operating systems and equipment; (vi) encrypting Personal Information stored on any mobile media; (vii) encrypting Personal Information in transit and at rest; (viii) strictly segregating Confidential Information from information of Receiving Party or its other customers so that Confidential Information is not commingled with any other types of information; (ix) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; (x) providing appropriate privacy and information security training to Receiving Party's employees; and (xi) ensuring Receiving Party's systems are properly patched and maintained.

(c) In the event of a Security Breach, Receiving Party shall: (i) provide Disclosing Party with the name and contact information for an employee of Receiving Party who shall serve as Disclosing Party's primary security contact and shall be available to assist Disclosing Party twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a Security Breach; (ii) notify Disclosing Party of a Security Breach without undue delay, but no later than seven (7) days after Receiving Party becomes aware of it; and (iii) notify Disclosing Party of any Security Breaches by phone and e-mail to Receiving Party's primary business contact within Disclosing Party. The notification obligation should include, to the extent possible, the identification of each individual whose Personal Information has been, or is reasonably believed by the Receiving Party to have been, accessed, acquired, used, or disclosed during the breach.

(d) Receiving Party shall use best efforts to immediately remedy any Security Breach and prevent any further Security Breach at Receiving Party's expense in accordance with applicable privacy rights, laws, regulations and standards.

(e) To the extent that the Receiving Party is authoring or modifying software code on behalf of Disclosing Party, the Receiving Party will ensure all of its coding personnel are trained in basic secure coding practices aligned with the Open Web Application Security Project (OWASP). To the extent that the Receiving Party is making privileged platform configuration changes, the Receiving Party will ensure those relevant personnel have appropriate security specific training on the platform. These training requirements will be completed by Receiving Party personnel prior to performing services for Disclosing Party and at the Receiving Party's expense. All Receiving Party's authored code and platform configurations will be tested by Disclosing Party for security defects prior to release. Any negligent practices that result in easily preventable security defects will be repaired by the Receiving Party at the Receiving Party's expense.

**4. Privacy and Security Audits.**

(a) Receiving Party shall employ ongoing oversight to the privacy and security obligations under the Agreement to ensure that internal controls are suitably designed and operating effectively to protect against reasonably foreseeable risks to Receiving Party data, including, but not limited to, auditing of the privacy and security safeguards based on recognized industry best practices. Upon Disclosing Party's request, no more than annually, Receiving Party must provide evidence that management oversight has occurred. Such evidence should briefly describe the oversight process, indicate whether Receiving Party's controls remain aligned to industry best practices, and include a signature of a corporate officer of the Receiving Party.

(b) Receiving Party is required to keep current the existing SSAE 18 Service Organization Control (SOC) report. This report, by SOC definition, must report on policies and procedures placed in operation and tests of operating effectiveness for a period of time. Reports must include the examination and confirmation steps involved related controls plus include an evaluation of the operating effectiveness of the controls for a period of at least six consecutive calendar months. SOC reports must be provided upon request.

(c) Where information is not already available in the above audit materials, Receiving Party will provide Disclosing Party, upon written request, with information that is needed to ensure that all terms of the Agreement are met.

**5. Deletion / Return of Confidential Information at Termination.**

At Disclosing Party's sole discretion and upon notification to Receiving Party, Receiving Party shall securely delete and/or return all Confidential Information in Receiving Party's possession within fifteen (15) days of the Agreement's termination using commercially acceptable methods.