Trusted Research Environment (TRE) Addendum

This Trusted Research Environment Addendum ("**Addendum**") is entered into by and between DNAnexus, Inc. ("**DNAnexus**") and the Customer specified in the applicable Order Form ("**Customer**") and modifies the Master Subscription Agreement ("**Agreement**") between the parties and having an Effective Date of specified in the applicable Order Form, as such Agreement amended in writing from time-to-time by the parties. Capitalized terms used but not defined herein shall have the meanings set forth in the Agreement.

1. Definitions.

1.1. "Data Exfiltration" means the unauthorized copying, downloading, manual transmission, or external removal of TRE Data or Customer Materials out of the TRE module environment via any vector path.

1.2. "TRE Data" means any Customer Data that is proprietary or regulated omics files, biometric datasets, clinical information, workflows, or analytical pipelines uploaded to, or generated within, a designated TRE project environment.

1.3. "Trusted Research Environment" or "TRE" means a specialized secure Module within the Service designated to permit controlled access to TRE Data and Customer Materials (including omics data).

1.4. "TRE Authorized User" means an individual researcher, collaborator, or institutional third party who has been provisioned with controlled access to a TRE project environment by or on behalf of Customer.

1.5. "Acceptable Use Policy for TRE" or "AUP for TRE" means DNAnexus' Acceptable Use Policy for Trusted Research Environments available at https://www.dnanexus.com/terms/tre-acceptable-use-policy.

2. Provision and Purpose of the TRE. DNAnexus may make available a secure environment within the Service designated as a Trusted Research Environment ("TRE"). The TRE is a Module designed to allow Customer to provision-controlled access to Customer Materials (including omics data) to designated TRE Authorized Users.

3. Customer Control and Access Governance. Customer maintains sole administrative control over the TRE. Customer is exclusively responsible for:

3.1. TRE Inventory. Configuring each TRE with an inventory of TRE Data.
3.2. **Provisioning Access.** Authenticating, provisioning, managing, and immediately de-provisioning TRE Authorized Users.
3.3. **Permissioning**. Configuring individual roles, data visibility, and computational tool permissions within the TRE.
3.4. **Security Setting.** Configuring security settings that control what is allowed and disallowed, or enabled and disabled, this includes egress route.
3.5. **Credential Security:** Ensuring all TRE Authorized Users utilize multi-factor authentication and maintain strict credential confidentiality.
3.6. **Data Access Requests.** Reviewing and approving data access requests of TRE Authorized Users.
3.7. **Compliance Oversight.** Monitoring TRE Authorized User activity to ensure absolute compliance with the AUP for TRE, Customer's internal governance, privacy policies, and all applicable Laws.

4. Refined Data Exfiltration Restrictions and Risk.

4.1. **Technical Controls.** The TRE incorporates specific technical controls designed to restrict Data Exfiltration via the Web UI, DNAnexus APIs, Client Software command-line scripts, automated API calls, or external platform integrations.
4.2. **No Absolute Guarantee**. Notwithstanding these controls, Customer explicitly acknowledges and agrees that DNAnexus does not warrant that the TRE will prevent all vector paths of Data Exfiltration (including visual capture, screenshots, photographs, manual transcription, or unblocked programmatic mechanisms, etc.).
4.3. **Assumption of Risk**. As between DNAnexus and Customer, Customer explicitly assumes all risk, liability, and consequences resulting from any authorized or unauthorized Data Exfiltration executed by a TRE Authorized User.
4.4. **Output Governance.** Customer is solely responsible for determining whether any analytical Output generated within a TRE Module may be safely Exported by TRE Authorized Users.

5. Compliance Logging and Audit Log Retention. To support regulatory compliance and forensic tracking, Customer may configure the Service to automatically generate and retain immutable audit trails of all activities inside the TRE.

5.1. **Log Capture.** DNAnexus may capture log data pertaining to all TRE Authorized User interactions, including login attempts, API calls, command execution, data access requests, configuration changes, and data export attempts.

5.2. **Retention Period**. DNAnexus may retain these TRE compliance logs for a minimum period of one (1) year from the date of generation.

5.3. **Customer Availability**. To the extent that DNAnexus has not already deleted such log data, DNAnexus will make these logs available to Customer upon Customer's reasonable written request to support Customer's internal compliance audits, regulatory reporting, or security investigations.

6. **Consumption and Usage Fees.** All cloud infrastructure, computational processing, and data storage resources utilized within the TRE generate operational expenses ("TRE Consumption Fees").

6.1. **Default Responsibility.** Except as otherwise explicitly structured in an applicable Order Form, Customer is solely responsible for the payment of all Consumption Fees incurred with respect to the TRE Module, including without limitation, activities of TRE Authorized Users within the TRE Module (such as the use of computational Tools, analysis of omics data, and storage of corresponding Output, etc.).

6.2. **Order Form Overrides.** Any arrangement to allocate or invoice Consumption Fees directly to a TRE Authorized User or a TRE Authorized User's underlying institution must be explicitly negotiated and set forth in a mutually executed Order Form referencing this Agreement. In the absence of such an Order Form provision, the Customer remains the default billing entity.

7. **Suspension of Access ("Kill Switch")**

7.1. Without limiting DNAnexus' holistic suspension rights under the Agreement, DNAnexus reserves the right to immediately suspend or terminate access to the Service for any individual TRE Authorized User, without liability to Customer, if DNAnexus is aware of or reasonably suspects a security vulnerability, compromised credential vector, or a violation of the AUP, the AUP for TRE, the terms of this Addendum, or applicable Law.

7.2. DNAnexus will use commercially reasonable efforts to provide prompt notice (email sufficient) to Customer's Administrator regarding any such individual user suspension.

8. **Responsibility for TRE User Actions.** Customer is fully responsible and liable for any and all actions, omissions, breaches of the AUP, or violations of Law committed by TRE Authorized Users within or relating to the TRE, as if such actions were taken directly by the Customer on Customer's Account.

9. **Dedicated TRE Indemnification.** In addition to the obligations set forth in the Agreement, Customer shall indemnify, defend, and hold harmless DNAnexus from and against any and all claims, costs, damages, losses, liabilities, and expenses (including reasonable attorneys' fees and costs) arising out of or relating to: (i) any unauthorized access, misuse, or Data Exfiltration of TRE Data or Customer Materials by a TRE Authorized User; or (ii) any data rights disputes or breaches of agreement occurring between Customer and a TRE Authorized User (or their underlying sponsoring institution).

10. **Effect of Addendum.** Except as expressly modified by this Addendum, all other terms and conditions of the Agreement shall remain in full force and effect. In the event of a direct conflict between the terms of this Addendum and the main body of the Agreement regarding the TRE Module, TRE Data, or TRE Authorized Users, the terms of this Addendum shall control.