DNAnexus DATA SECURITY

1.1 **Environment**. DNAnexus shall securely process, host, transmit, and store the Customer Data. DNAnexus shall provide the Service using no less than generally accepted industry practice physical and environmental security measures designed to prevent unauthorized access to, theft of, or unlawful disclosure of the Customer Data. DNAnexus shall employ technologies that are consistent with industry standards for firewalls and other security technologies. DNAnexus shall notify Customer of each location for storing data.

1.2 **Data Transfers**. DNAnexus shall use Secure Sockets Layer ("SSL") standards, or then-current successor protocols, designed to protect data confidentiality during transfers. In addition, DNAnexus shall maintain at a minimum the following security measures: HTTP with SSL 256-bit encryption ("HTTPS"); at least 256-bit AES encryption and encode data during transmission; and encrypted passwords for hosting services.

1.3 **Information Security Program.** DNAnexus shall establish, implement, and maintain an information security program that includes technical and organizational security and physical measures as well as policies and procedures designed to protect Customer Data processed by DNAnexus against accidental loss; destruction or alteration; unauthorized disclosure or access; or unlawful destruction. DNAnexus' information security program must reasonably address the confidentiality, integrity, and availability of all Customer Data, including the below matters and any other requirements specified in this attachment:

A. Periodic risk assessments.

B. Identification and documentation of the security requirements of authorized users.

C. User access, the nature of that access, and authorization of access.

D. Prevention of unauthorized access through the use of effective physical and logical access controls.

E. Procedures to manage system-level access.

F. Assignment of responsibility and accountability for security and for system changes and maintenance.

G. Implementation of system software upgrades and patches, including a patching review interval of once per calendar quarter for security impacting patches. In addition to this regular patching review schedule, DNAnexus shall implement appropriate patches if it becomes aware at any time of a security vulnerability and DNAnexus shall implement critical patches as soon as possible.

H. Testing, evaluating, and authorizing system components before implementation.

I. Resolution of complaints and requests relating to security issues.

J. Handling of errors and omissions, security breaches, and other incidents.

K. Procedures to detect actual and attempted attacks or intrusions into systems and to proactively test security procedures (for example, penetration testing).

L. Allocation of training and other resources to support its security policies.

M. Risk and security incident management.

N. Processing integrity and related system security policies.

O. A requirement that users, management, and third parties confirm (initially and annually) their understanding of an agreement to comply with the applicable privacy policies and procedures related to the security of Customer Data.

P. Procedures for proper destruction and disposal of Customer Data.

1.4 **Report**. On an annual basis upon request, DNAnexus shall provide Customer an appropriate report such as the ISO/IEC 27001 certification across all controls in ISO/IEC 27002 (or comparable). The audit will be conducted by a third-party audit firm with appropriate expertise. The audit will be specific to the DNAnexus Platform. On an annual basis upon request, DNAnexus shall give Customer a full copy of the report. Upon written request from Customer, DNAnexus shall also give Customer a management representation letter stating that, to the knowledge of DNAnexus management after reasonable investigation, there have been no changes to the control environment between the date of the management representation letter and the date of the audit.

1.5 **Audit and Test**. Customer may conduct non-intrusive network audits (basic port scans, etc.) with reasonable prior notice. Customer shall not attempt to access the data of another DNAnexus customer. Customer may perform any technical security integrity review, penetration test, load test, denial-of-service simulation or vulnerability scan with DNAnexus' prior written consent.

1.6 **Mitigation of Vulnerabilities.** DNAnexus shall promptly mitigate any critical security vulnerabilities discovered at any time.

1.7 **Notification of Security Breach.** Upon becoming aware of any unlawful or unauthorized access to any Customer Data stored on DNAnexus' equipment or in DNAnexus' facilities, or any unauthorized access to any facilities or equipment resulting in loss, disclosure, or alteration of any Customer Data, or any actual loss of or suspected threats to the security of Customer Data, DNAnexus personnel will immediately:

A. notify Customer's Information Security Department of the incident;

B. investigate and provide assistance in the investigation of the security incident by conducting a through root-cause analysis, producing a report of such analysis and providing such report to Customer;

C. provide Customer with detailed information about the security incident;

D. take all commercially reasonable steps to mitigate the effects of the security incident and providing a report of such mitigation efforts to Customer; and

E. implement a remediation plan and monitor the resolution of breaches and vulnerabilities related to Customer Data to ensure that appropriate corrective action is taken on a timely basis.

1.8 **Reporting**. DNAnexus shall provide a preliminary report of all issues related to security breaches to Customer's Information Security department within 24 hours after discovery and a final report promptly upon completion of investigation. DNAnexus shall provide prior notice to Customer of any proposed communications to third parties related to any security incident and will work on them in coordination with Customer. DNAnexus shall not issue any communication without Customer's approval unless required by applicable law.

1.9 **Business Continuity Plan**. DNAnexus shall establish, implement, test, and maintain an effective business continuity plan (including without limitation disaster recovery and crisis management procedures) to provide continuous access to, and support for the Services to Customer. DNAnexus shall perform backup and disaster-recovery planning processes designed to protect Customer Data from unauthorized use, access, disclosure, alteration, or destruction.

1.10 **Backup and Archives**. DNAnexus shall back up, archive, and maintain duplicate or redundant systems that can fully recover all Customer Data on a daily basis. DNAnexus shall establish and follow procedures and frequency intervals for transmitting backup data and systems to DNAnexus' backup location. DNAnexus shall maintain the backup storage and systems in a secure physical location other than the location of DNAnexus' primary systems. DNAnexus shall update and test the backup storage systems at least annually. Upon written request, DNAnexus shall provide Customer with a summary of DNAnexus' business continuity plan.

1.11 **Confidentiality and Compliance**. Customer shall maintain the confidentiality of the reports it reviews. Customer shall comply with all applicable laws and regulations, including to the Fair Credit Reporting Act and data protection and privacy regulations when acting pursuant to this Agreement.

1.12 **Network Security**. DNAnexus shall configure its network infrastructure to enforce the "principle of least access," including filters that allow only the minimum required traffic.

1.13 **Host Monitoring**. Upon written request, DNAnexus shall disclose the high level processes for monitoring the integrity and availability of the hosts.

1.14 **Passwords**. DNAnexus shall store any passwords within a secured database server, using industry standard security measures behind DNAnexus' firewall. DNAnexus shall use SHA-256 or higher to scramble or hash the database password. DNAnexus' system must require this password upon application startup to connect to the database.

1.15 **Web Security**. DNAnexus shall provide Customer with the process for doing quality assurance testing for the application, for example, testing of authentication, authorization, and accounting functions, as well as any other activity designed to validate the architecture.

1.16 **Encryption Algorithms**. DNAnexus shall use cryptographic algorithms that have been published and evaluated by the general cryptographic community. DNAnexus shall use encryption algorithms that are sufficient strength to equate to 256-bit or better. DNAnexus may use hashing functions SHA-256 or higher. DNAnexus shall not use any "homegrown" cryptography, such as symmetric, asymmetric, or hashing algorithm.

1.17 **Encryption Key Management**. DNAnexus shall provide encryption key management. DNAnexus shall protect private keys in storage, transit, and backup. A separate key per customer is preferred instead of a global key for all customers. DNAnexus shall segregate the encryption key and encryption key management process from any hosts that store and process the data. DNAnexus shall provide Customer with documentation of its security controls for the secure key management. DNAnexus shall provide an effective key destruction technique, such as crypto shredding, to ensure that the encryption keys are destroyed and unrecoverable after the Agreement is terminated.

1.18 **Identity Provisioning and De-provisioning**. DNAnexus shall provide a secure and timely management of on-boarding and off-boarding of cloud service users. DNAnexus shall use standard APIs, such as Simple Cloud Identity Management.

1.19 **Federation**. If within the scope of the applicable SOW, DNAnexus shall use Customer's single sign-on mechanisms which include the SAML v2 federation standard.

1.20 **Strong Authentication**. DNAnexus shall use two-factor authentication and certificates to authenticate their remote administrators who manage their cloud services, or an alternative strong authentication method.

1.21 **Authorization and Access Controls**. DNAnexus shall maintain a policy and role-based access control model to log user access information for compliance audit and incident investigation purposes.