DNAnexus

DNAnexus, Inc.
DATA AND SECURITY POLICY
(Revised as of June 27, 2022)

Introduction

At DNAnexus we take the protection of Customer Data extremely seriously. This Data and Security Policy ("**Policy**") describes the organizational and platform-wide technical measures implemented by DNAnexus that are designed to prevent unauthorized access, use, alteration or disclosure of Customer Data. The DNAnexus Service operates on Amazon Web Services ("**AWS**") or Microsoft Azure ("**Azure**") as selected by Customer (collectively, the "**Infrastructure Providers**"); this Policy describes activities of DNAnexus within its instance on the applicable Infrastructure Provider unless otherwise specified.

Capitalized terms used but not defined in this Policy will have the meanings set forth in the DNAnexus online "**Subscription Terms of Service**" (https://www.dnanexus.com/terms) or in the Master Subscription Agreement between DNAnexus and you ("**Customer**") under which Customer is granted access to the DNAnexus Service ("**Agreement**"). In the event of any conflict or inconsistency between the Agreement and this Policy, this Policy will control.

1. General Security Features of the DNAnexus Service

1.1. Industry standard virtual firewall and other security technologies.

1.2. Network infrastructure for DNAnexus instances designed with physical and logical access controls based on the "principle of least access," including filters that allow only the minimum required traffic.

1.3. Procedures to manage system-level access.

1.4. Policy and role-based access control model to log User access information for compliance audit and incident investigation purposes.

1.5. Two-factor authentication and certificates (or an alternative strong authentication method) to authenticate DNAnexus' remote administrators who manage the DNAnexus Service.

1.6. 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, if DNAnexus becomes aware at any time of a security vulnerability with the DNAnexus Service, DNAnexus shall implement appropriate patches promptly and in the case of critical patches, as soon as possible.

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

1.8. Periodic risk assessments and other procedures designed to detect actual and attempted attacks or intrusions into systems and to proactively test security procedures (for example, penetration testing).

1.9. Destruction and disposal of Customer Data in accordance with applicable industry standards, such as the DoD 5220.22-M, FIPS 800-88, and DIN 66399 standards for data sanitation.

2. Encryption

2.1. Encryption Algorithms. DNAnexus uses cryptographic algorithms that have been published and evaluated by the general cryptographic community to encrypt Customer Data at rest and in transit. DNAnexus shall use encryption algorithms that have at least 256-bit key lengths (or the cryptographic equivalent).

2.2. Data Transfers. DNAnexus uses Secure Sockets Layer (SSL) standards, or then-current successor protocols, designed to protect Customer Data from unauthorized access during transfers to and from the DNAnexus Service. Each SSL connection will use at least AES-256 encryption. All HTTP communications will use SSL connections via the HTTPS protocol.

2.3. Passwords. DNAnexus stores User passwords within a secured database server hosted on the applicable Infrastructure Provider, using industry standard security measures behind DNAnexus' firewall. DNAnexus uses SHA-256 or another hashing function of at least equivalent strength to scramble or hash the password database. The DNAnexus Service requires passwords upon startup to connect to Customer's Account. Alternatively, customers may configure their org to use their own Single Sign On (SSO), whereupon the password complexity and multifactor authentication is the responsibility of the customer.

2.4. Encryption Key Management. DNAnexus uses commercially reasonable encryption key management procedures, including maintaining customer-specific encryption keys and logically segregating encryption keys from encrypted Customer Data. Upon Customer's request, no more than one time per year, DNAnexus shall provide documentation of its security controls for encryption key management. DNAnexus shall utilize an effective key destruction technique, such as crypto shredding, to ensure that the encryption keys are destroyed and unrecoverable after the Agreement is terminated.

3. Certifications

3.1. DNAnexus is ISO 27001 certified with ISO 27002 controls.

3.2. DNAnexus has FedRAMP "**Authority to Operate**" at Moderate renewed on 03-Jan-2022.

3.3. When engaging in certain data transfers between the EEA and other countries, DNAnexus enters into Standard Contractual Clauses following the invalidation of the EU-US Privacy Shield. DNAnexus views itself as a Data Processor under GDPR.

4. DNAnexus Information Security Program

4.1. DNAnexus maintains an internal Information Security Program consistent with this Policy.

4.2. DNAnexus requires its personnel with access to Customer Data to confirm (on an annual basis) that they will comply with all applicable DNAnexus policies related to security of Customer Data.

4.3. DNAnexus allocates training and other resources to support compliance with its Information Security, Privacy and Quality Programs as well as the DNAnexus Code of Conduct

5. Business Continuity Plan

5.1. DNAnexus shall establish, implement, test, and maintain a business continuity plan (including without limitation disaster recovery and crisis management procedures) to provide continued access to, and support for the DNAnexus Service to Customer. Upon Customer's request, no more than one time per year, DNAnexus will provide a written summary of DNAnexus' Business Continuity Plan, including confirmation that it has successfully tested the Business Continuity Plan.

5.2. The Recovery Time Objective (RTO) of the DNAnexus Service is 8 hours. The Recovery Point Objective (RPO) is 4 hours.

5.3. Customer is responsible for the backup and recovery of objects in its Account on the DNAnexus Service platform.

6. Incident Response

6.1. <u>Mitigation of Vulnerabilities</u>. DNAnexus shall promptly commence mitigating any critical security or privacy vulnerabilities upon discovery.

6.2. <u>Notification of Security or Privacy Breach</u>. Upon becoming aware of any unauthorized access to any Customer Data stored in the DNAnexus Service, DNAnexus will promptly:

6.2.1. notify Customer's Information Security and/or Privacy Department of the incident;

6.2.2. investigate the incident by conducting a through root-cause analysis, producing a report of such analysis and providing such report to Customer upon conclusion of its investigation;

6.2.3. provide Customer with detailed information about the incident;

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

6.2.5. 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.

6.3. <u>Communications with Third Parties</u>. Where legally permitted, DNAnexus shall provide prior notice to Customer of any proposed communications to third parties related to any security incident involving Customer Data and will reasonably coordinate with Customer regarding such communications. DNAnexus shall not issue any public communication regarding any security incident involving Customer Data that identifies Customer without Customer's approval unless required by applicable law.

7. Audits

7.1. <u>Audits</u>. DNAnexus commissions annual independent audits of its ISO 27001 and FedRAMP controls. The audit is specific to the DNAnexus Service.

7.2. <u>Reports</u>. On an annual basis upon Customer's request, DNAnexus shall provide Customer a summary of its most recent third-party audit report documenting DNAnexus' compliance with its certifications and controls.

7.3. <u>Customer Tests</u>. Customer may conduct non-intrusive network tests of the DNAnexus Service (specifically, basic port scans or similar tests that do not require authentication or login) with reasonable prior notice and DNAnexus' consent (which DNAnexus may withhold in its sole discretion). Customer is strictly prohibited from performing any load test, denial-of-service simulation or vulnerability scan. At no time may Customer attempt to access the data or account of another DNAnexus customer.

8. Infrastructure Providers

8.1. The DNAnexus Service is hosted on infrastructure of the Infrastructure Provider listed in the applicable Order Form in the region specified in the applicable Order Form.

8.2. The DNAnexus Service builds on the physical security and environmental controls provided by its Infrastructure Providers.

8.2.1. See https://aws.amazon.com/security/ for details of AWS security infrastructure and information about AWS security certifications and obtaining copies of security reports.

8.2.2. See https://docs.microsoft.com/en-us/azure/security/azure-security for details of Azure security infrastructure and information about Azure security certifications and obtaining copies of security reports.

9. Customer Responsibilities

9.1. Confidentiality. All reports provided by DNAnexus are "DNAnexus Confidential". Customer shall maintain the confidentiality of such reports.

9.2. Compliance. Customer is responsible for complying with the terms of Customer's Agreement with DNAnexus, including compliance with all applicable laws and regulations.

9.3. Access Permissions and Account De-provisioning. Customer is responsible for managing its own User accounts and roles from within the DNAnexus Service, including de-provisioning User access.

9.4. Credentials. Customer is responsible for protecting its own Account and User credentials by using multi-factor authentication and industry standard password complexity protocols for all Users and promptly notifying DNAnexus if a User credential has been compromised.

9.5. Backup and Archives. Customer is responsible for maintaining backups and archives of all Customer Data input into the DNAnexus Service.

9.6. Malware. Customer is responsible for scanning all Customer Tools for the presence of viruses, malware and other harmful code.

9.7. Security/Privacy Threats. Customer is responsible for promptly notifying DNAnexus if Customer suspects possible suspicious activities or security/privacy threats that could negatively impact security of the DNAnexus Service, Customer Data or Customer's Account.