Nuix Security Requirements

1. **General**. Nuix must establish and maintain reasonable physical, technical, and administrative safeguards, designed to prevent the unauthorised access, use, disclosure, or alteration of Customer Data processed using the SaaS Offering. Such procedures and safeguards must comply with applicable Laws and must be no less rigorous than those maintained by Nuix for its own information of a similar nature. Nuix must regularly, but in no event less than annually, evaluate the effectiveness of its information security program and must adjust and update such program in consideration of the results of such evaluation.
2. **Policies and Procedures**. Nuix must maintain written internal information security policies and procedures as part of its information security program. Such policies may include requirements and procedures relating to acceptable use of assets, passwords, secure development and engineering, information asset handling, media disposal, event, and system logging, change control, security incident response, business continuity, and disaster recovery.
3. **Security Certifications**. For SaaS Offerings, Nuix must comply with and annually obtain a third party audit report assessing its compliance with the then-current version of ISO/IEC 27001 – Information Security Management, for the cloud-based infrastructure supporting its SaaS Offering, covering: (a) the native client applications; (b) the web applications and services; (c) application programming interfaces; (d) software development lifecycle; and (e) source code, as these relate to the Solution.
4. **Access Controls**. Nuix must implement and maintain reasonable access controls, including authentication and password requirements, and remote access policies, applicable to media, applications, operating systems, and equipment controlled by Nuix in processing Customer Data. Nuix must restrict access to records and files containing Customer Data to those personnel who need to know such information to perform their job duties.
5. **SaaS Offerings Security**. Nuix must implement reasonable measures to secure its SaaS Offerings. These measures may include, but are not limited to, implementing software and security patches and updates, firewalls, up-to-date anti-virus software, intrusion detection and prevention mechanisms and technologies, and technologies for monitoring and logging the processing of Customer Data (including outside of normal system activity).
6. **Segmentation**. Nuix must logically separate Customer Data from Nuix's other customer data in its SaaS Offering. Customer databases and customer file shares are logically separated and dedicated for each customer organisation within the SaaS Offering.
7. **Encryption**. Nuix must encrypt Customer Data: (a) at rest, within the SaaS Offering boundary, and (b) in transit, to and from the SaaS Offering boundary, using reasonable encryption technologies (to AES-256). "**SaaS Offering boundary**" means the logical and physical demarcation point at which Customer Data enters or leaves the Nuix-controlled SaaS Offering environment.
8. **Data Back-up, Recovery and Destruction Procedures**. Nuix will implement and maintain industry-standard back-up and recovery procedures for SaaS Offerings, including to accommodate a Recovery Objective Time (RTO) of 4 hours and Recovery Objective Point (RPO) of 1 hour. Nuix's obligations in respect of loss, corruption, or destruction of Customer Data in any SaaS Offering are limited to using commercially reasonable efforts to restore Customer Data from the most recent back up available. The Customer is otherwise responsible and liable for storage and back-up of Customer Data in relation to SaaS Offerings. Any Customer Data that is to be deleted from the SaaS Offering will be deleted or destroyed using appropriate commercially reasonable methods. Nuix is not required to remove residual copies of data from backup or disaster recovery systems, provided such copies are not accessible in the ordinary course of business.
9. **Employee Matters**. Nuix must provide its personnel who have access to Customer Data with information security training designed to ensure such employees' compliance with Nuix's contractual and legal obligations in relation to Customer Data. In addition, Nuix must ensure that employees with access to Customer Data are subject to confidentiality obligations protecting the confidentiality of such data. Nuix must conduct such background checks on Nuix employees as Nuix deems appropriate for the employee's role, to the extent permitted by applicable Law.
10. **Service Provider Controls**. Nuix must require that service providers processing Customer Data on Nuix's behalf maintain reasonable safeguards to protect such Customer Data.
11. **Physical Security**. Nuix must maintain reasonable physical security at facilities controlled and operated by Nuix ("**Nuix Facilities**") appropriate to Nuix's use of those facilities. Physical security controls at Nuix Facilities must include the following, at a minimum:
    (a) all entrances and exits to Nuix Facilities must be equipped with alarms designed to detect and alert security personnel to unauthorised access;
    (b) access to Nuix Facilities must be by key-card or equivalent method that authenticates individuals and logs all entries;
    (c) visitors to Nuix Facilities must be clearly identified and their access limited only to areas necessary to fulfill their functions; and
    (d) Nuix must maintain access logs of Nuix employees and visitors who have gained access to the Nuix Facilities.

12. **Data Centres**. Nuix relies on third party data centre providers (currently AWS and Zadara) to supply the physical infrastructure and physical security at to process Customer Data in Nuix's SaaS Offerings. Information concerning AWS's physical security controls may be found at https://aws.amazon.com/compliance/data-center/controls/. Information concerning Zadara's physical security controls can be found at: https://support.zadarastorage.com/hc/en-us/articles/213025226-Zadara-Storage-Security-Brief.

13. **Definitions**. In these Security Requirements:

    Customer Data means all electronic documents and information submitted to or generated by Software or a SaaS Offering by or on behalf of Customer.

    SaaS Offering means the software-as-a-service offerings hosted and made available by Nuix to Customer.

    Software means the object code version of any software supplied by Nuix to Customer for use in an environment managed or controlled by Customer.