Security Policy

Last Update : July 16, 2020

Please be informed that this security policy document ("**Security Policy**") is part of our Privacy Policy.

The security of your Personal Information is important to us. We seek to protect your Personal Data from unauthorized access, use and disclosure using appropriate physical, technical, organizational and administrative security measures based on the type of Personal Information and how we are processing that data. We endeavour to follow generally accepted industry standards to protect the Personal Information submitted to us, both during transmission and in storage.

Moreover, you should also help us in protecting your Personal Information by appropriately selecting and protecting your password and/or other sign-on mechanism; limiting access to your computer or device and browser; and signing off after you have finished accessing your account. Although we work to protect the security of your account and other data that we hold in our records (for example by making good faith efforts to store Personal Information in a secure operating environment that is not open to the public), please be aware that no method of transmitting data over the Internet or storing data is completely secure. We cannot and do not guarantee the complete security of any data shared with us, and except as expressly required by law, we are not responsible for the theft, destruction, loss or inadvertent disclosure of your information or content. If at any time during or after our relationship we believe that the security of your Personal Data may have been compromised, we may seek to notify you or the Third-Party User that provided us with your Personal Data of that development. If a notification is appropriate, we will endeavour to notify you or such Third-Party User as promptly as possible under the circumstances. If we have your email address, we may notify you by email to the most recent email address you have provided us in your account profile. Please keep your email address in your account up to date. You can update that email address anytime in your account profile. If you receive a notice from us, you can print it to retain a copy of it. To receive these notices, you must check your email account using your computer or mobile device and email application software. You consent to our use of email as a means of such notification

Therefore, this document is intended to indicate to you how the measures we take to protect you when you are using Nodeflux Services.

Confidentiality

We place strict controls over our employees' access to the data you and your users make available via the Nodeflux services, as more specifically defined in your agreement with Nodeflux covering the use of the Nodeflux services (**"Customer Data"**). The operation of the Nodeflux services requires that some employees have access to the systems which store and process Customer Data. For example, in order to diagnose a problem you are having with the Nodeflux services, we may need to access your Customer Data. These employees are prohibited from using these permissions to view Customer Data unless it is necessary to do so. We have technical controls and audit/logging system in place to ensure that any access to Customer Data is logged.

Data Encryption In Transmissionand At Rest

We use at-rest data encryption in infrastructure level using state of the art key management system and industry proven cipher suites and protocols. For detailed how we use data encryption at rest you can click here

For Data Encryption in transmission, we use SSL/TLS encryption supporting the latest **TLS 1.3** version. The data stream is encrypted with **AES 256** that gives highest security protection without sacrificing performance.

We monitor the changing cryptographic landscape closely and work promptly to upgrade the service to respond to new cryptographic weaknesses as they are discovered and implement best practices as they evolve. For encryption in transit, we do this while also balancing the need for compatibility for older clients.

Availability

We understand that you rely on the Nodeflux services to work. We're committed to making Nodeflux a highly-available service that you can count on. Our infrastructure runs on systems that are fault tolerant, for failures of individual servers or even entire data centers. Our operations team tests disaster-recovery measures regularly and staffs an around-the-clock on-call team to quickly resolve unexpected incidents.

Disaster Recovery

Customer Data is stored redundantly at multiple locations in our hosting provider's data centers to ensure availability. We have well-tested backup and restoration procedures, which allow recovery from a major disaster. Customer Data and our source code are automatically backed up nightly. The Operations team is alerted in case of a failure with this system. Backups are fully tested at least every 90 days to confirm that our processes and tools work as expected.

Logging

Nodeflux maintains an extensive, centralized logging environment in its production environment which contains information pertaining to security, monitoring, availability, access, and other metrics about the Nodeflux services. These logs are analyzed for security events via automated monitoring software, overseen by the security team.

Incident Management & Response

In the event of a security breach, Nodeflux will promptly notify you of any unauthorized access to your Customer Data. Nodeflux has incident management policies and procedures in place to handle such an event.

External Security Audits

We contract with respected external security firms who perform regular audits of the Nodeflux services to verify that our security practices are sound and to monitor the Nodeflux services for new vulnerabilities discovered by the security research community. In addition to periodic and targeted audits of the Nodeflux services and features, we also employ the use of continuous hybrid automated scanning of our web platform.

Compliance

The following security-related audits and certifications are applicable to the Nodeflux services:

- Nodeflux has achieved **ISO 27001** compliance. You can download the ISO 27001 certificate here A copy of the Statement of Applicability is available upon request from your Account Manager.

The environment that hosts the Nodeflux services maintains multiple certifications for its data centers, for more information about their certification and compliance, please visit the AWS

Security website, AWS Compliance website, Google Security website, and Google Compliance website.