Nimonik

info@nimonik.com 1-888-608-7511

Last Updated: March 15th, 2017

Nimonik Inc. takes data security very seriously. Our clients around the world collect and manage sensitive information and we pride ourselves on strict security settings that are both safe and cost effective for all of our clients. Below are some technical and administrative details, for more information please contact us at info@nimonik.com

**Administrative controls**

Only three people in the Nimonik organization have access to client data, our CEO, our CTO and a System Administrator. If a client requires assistance in their account, they must give Nimonik staff explicit permission to access their account data for the purpose of the support ticket. The client can revoke access at anytime.

**Technical controls**

- Nimonik undergoes regular Penetration (PEN) Tests, reports can be provided on request.
- Nimonik has Network Intrusion Detection Systems and Network Intrusion Prevention Systems.
- NimonikApp is hosted on Amazon AWS, which follows leading industry standards. https://aws.amazon.com/security/ in Virginia, United States.
- Nimonik date is encrypted at Rest using Amazon AWS RDS. (https://aws.amazon.com/kms/details/#secured & http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html)
- Backups are stored and encrypted using SSE-S3 encryption method. They are stored on Amazon servers in the United States (us-east-1 in North Virginia).
- Nimonik uses secure HTTPS protocol by default and redirect to it if user tries to access the app via the unsecure HTTP; the API calls are also always HTTPS; this way no data can be hijacked in transport. Nimonik uses an up-to-date version of SSL
- We use industry standard authentication with DB-hashed passwords. We use the bcrypt hashing function that https://en.wikipedia.org/wiki/Bcrypt
- Authorization mechanisms allow limiting access to parts of the site and to particular data.
- All pages and database queries are strictly limited to current user's account - there is no way to access another company's records.
- Our content administrators can only access company and user information; no sensitive data from the account is accessible from the admin panels.
- Sensitive data is filtered from logs and notification systems on a per user basis.
- The web framework we use (Ruby on Rails) automatically deals with dangers such as XSS/SQL injections.
- We keep our infrastructure up-to-date with security fixes (Ubuntu, Ruby, Rails, etc.).
- We do not store credit card information - we use Recurly (http://recurly.com) to keep billing info safe. Recurly is PCI Compliant https://recurly.com/security.
- Nimonik has a quick action plan for responding to attacks (e.g. DDOS) and Amazon AWS has a number of protections against a variety of attacks.
- Nimonik regularly conducts automated penetration tests and is working towards ISO 27001 certification by end of 2017.
- Nimonik offers Multi-Factor Authentication (MFA) with tokens sent to mobile phones.
- Passwords must contain 1 numeral, 2 alpha characters and at least one Capital letter.

- Passwords can optionally be reset every 90 days.

Some of our current Fortune 500 clients include Abbott Point of Care, United Technologies, L'Oréal, DeBeers Mining, Rio Tinto IOC, Glencore, FedEx BHP Billiton, VALE Mining and many others.

Sincerely,

Jonathan Brun, CEO, 514-712-0637