

DATANET SECURITY

2009-02-25

DataNet is TRAFx Research Ltd.'s (TRAFx) online, hosted software solution to analyze, manage, store and share TRAFx data. We know that you expect the DataNet service to be available to you when you login, and that you also expect a high standard of security. For the peace of mind of our DataNet customers, we take various measures to meet these availability and security expectations.

We work with Amazon Web Services (part of the well-known Amazon.com company) to provide you the DataNet service, and to securely backup your data. Amazon Web Services (AWS) is a highly scalable cloud computing platform with high availability and dependability.

Service Provision

DataNet is hosted on Amazon Elastic Compute Cloud (Amazon EC2), Amazon's proven computing environment. This service is fully scalable, and enables TRAFx, if necessary, to increase or decrease capacity quickly by commissioning one or more server instances; replacement instances can be added rapidly and predictably. The service runs within Amazon's proven network infrastructure and datacenters.

Physical Security

Amazon has many years of experience in designing, constructing, and operating large-scale data centers. AWS data centers are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication no fewer than three times to access Amazon Web Services Security data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

Secure Socket Layer (SSL)

For DataNet, we recommend you use Microsoft Internet Explorer 6.0 (released 2001) or later, or Firefox 2.0 (released 2006) or later). When you access DataNet using these browsers, Secure Socket Layer (SSL) technology protects information using both server authentication and data encryption to help ensure that data is safe and secure.

Secure Logins

Unique user names and passwords must be entered each time a customer logs in to DataNet. These safeguards help prevent unauthorized access, maintain data accuracy, and ensure the appropriate use of data.

Your password is encrypted before it is stored in our database. At no point can another person retrieve your password (TRAFx staff included). Nor does an administrator have the ability to set your password to a known value.

If you forget your password, or repeatedly try to log in with an incorrect password, your DataNet account will be locked for a 24 hour period. This helps prevent automated "dictionary" attacks against your account.

Data Backup

Data is backed up and stored in at least two geographically-separate, secure locations, within the Amazon system.

TRAFx makes twice daily backups of the DataNet database which we store on Amazon S3 (<http://aws.amazon.com/s3/faqs/>). All backups done by TRAFx that we store on Amazon S3 are full backups. We keep 2 weeks worth of twice daily full backups, plus backups from the 1st and 15th for at least 6 months. All backups placed on Amazon S3 are encrypted.

Defence/Intrusion protection

Amazon EC2 provides a complete firewall solution. The AWS network provides significant protection against traditional network security issues.

From time to time, we may make changes to this DataNet Security document. We will post the date of modification at the top of this document. We strongly encourage you to refer back to this document periodically.