STR8LINE SECURITY STATEMENT FOR CLOUD COMPUTING

For the use of STR8LINE App's, web applications,
API's, forms, portals and widgets

Last Updated: November 2012 (second version)

Content

Introduction

In the early 2000s, the Pentagon developed a protocol that guarantees the security of data in public networks such as the world-wide web (internet), the so-called SAS70 protopcol.

SAS70 is now the most accepted standard in the world for the computer systems and networks in the area of security. This also satisfies GDPR General Data Protection Regulation. (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas.

STR8LINE is SAS70 compliant.

About this statement

We use English for our privacy policy, please ask for a translation your local STR8LINE vendor or distributor.

This Security Statement applies to information, through your use of STR8LINE's Services. By using STR8LINE's Services and accepting the End User Agreement, as applicable, you also agree to this Security Statement. If you do not agree to this Security Statement, you must not use STR8LINE's Services. The terms "We," "Us," "Our," or our affiliates, platform partners that are using the STR8LINE engine as a white label (powered by STR8LINE). It explains how we secure our Cloud computing platform.

Scope on safe and secure Cloud Computing
All of the information we collect we secure, including:

- SSL
- High availability
- GDPR
- Backup and recovory protocol
- Sources Code Escrow
- Securing crypto computing and Blockchain
- API security

What is an SSL Certificate?

SSL Certificates are small data files that digitally bind a cryptographic key to an organization's details. When installed on a web server, it activates the padlock and the https protocol and allows secure connections from a web server to a browser. Typically, SSL is used to secure credit card transactions, data transfer and logins, and more recently is becoming the norm when securing browsing of social media sites.

SSL Certificates bind together:

1. A domain name, server name or hostname.
2. An organizational identity (i.e. company name) and location.

How we use SSL

Using insecure and deprecated security policies for your Juno cloud computing products SSL negotiation configuration will have a clear way of understanding what the Diffie-Hellman key exchange (DHE) has been like. deployed and FREAK Attack, which allows an attacker to intercept HTTPS connections between vulnerable clients and servers / load balancers in order to break in and steal or manipulate sensitive data. To maintain your Juno cloud computing products SSL configuration secure, Cloud Conformity recommends using the latest Predefined Security Policies released by Amazon Webservices (AWS).

What is High Availability?

High availability is a characteristic of a system, which aims to ensure an agreed level of operational performance, usually uptime, for a higher than normal period.

Modernization has resulted in an increased reliance on these systems. For example, hospitals and data centers require high availability of their systems to perform routine daily activities. Availability refers to the ability of the user community to obtain a service or good, access the system, whether to submit new work, update or alter existing work, or collect the results of previous work. If a user cannot access the system, it is – from the users point of view – unavailable. Generally, the term downtime is used to refer to periods when a system is unavailable.

What level we guarantee

Availability %	:	99.999% ("five nines")
Downtime per year	:	5.26 minutes
Downtime per month	:	26.30 seconds
Downtime per week	:	6.05 seconds
Downtime per day	:	864.00 milliseconds

Downtime is measured per year. Time calculations per month, week and day are averages.

What we do to maintain High Availability

1. Application-Level Routing

In the event of a transaction failure, cloud-aware applications can be engineered to intelligently route transactions to a secondary service point. A failed transaction query is automatically reprocessed at the secondary working location.

2. Network IP Management

Network IP Management allows a published service IP to move between machines at the time of a failure. This is classified as a self-healing process, where two servers monitor one another. If the first server malfunctions, the second server assumes its roles and processes.

3. Monitoring

A well-integrated monitoring package not only provides insight into an application and its current function, it monitors error-rates that exceed a predefined threshold. For example, an e-commerce site can set up monitoring on a payment gateway so that if credit card authorization transactions exceed a 20% failure rate, their Network Operations Center (NOC) automatically gets an alert and self-healing tasks on the infrastructure initiate.

4. Stateless Transactions

Engineering an application to perform transactions in a stateless manner significantly improves availability. In a stateless model, any machine only keeps state (data on) transactions that are 'in fly,' but after a transaction is completed, any machines that die or degrade have no effect on the state or memory of historic transactions. Clients are therefore not limited to server dependence, and the loss of any pool member in a tier ensures the client session is not interrupted due to a hardware or application fault on a discrete pool member.

5. Multi-Site Configurations

In the (unlikely) event of a catastrophic hardware failure, resources can be redeployed to a secondary location in minutes and with little planning. Data replication and resource availability is present in the secondary location, and the just-in-time deployment of entire application infrastructures is measured in minutes, not hours or longer.
When architected and implemented properly, multi-site configurations allow a company to redeploy their entire infrastructure in a new data center.
An organization that cannot tolerate downtime in their application infrastructure will benefit the most from a multi-site configuration. In this situation, the additional site would be a completely independent data center that hosts an independent copy of the primary site infrastructure. Depending on how the site application is configured, the additional site can either be in an active-active configuration that services a portion of the traffic coming into the site, or a primary-failover site that will not serve traffic, but sits idle while continuously replicating data from the primary.

A very urgent and critical problem that literally blocks the operation of a customer is not affecting downtime guarantee, as it is not creating downtime of the server. At Juno these are processed according to protocols within 30 minutes and immediately resolved.

What is Back-up and recovery?

Backup and recovery refers to the process of backing up data in case of a loss and setting up systems that allow that data recovery due to data loss. Backing up data requires copying and archiving computer data, so that it is accessible in case of data deletion or corruption.

How we gurantee back-ups and test recovery

With our BladeVPS services we take snapshots every week. This is an image of the complete data that is currently on the server. Because we only have access to the data on 'blocklevel' and not to 'file level', it is not possible to restore individual files from this. Replacing a snapshot always resets all data.
Also we do back-ups automatically every 5 minutes of all files, storing these (at least) 1 month. Recovery tests are taking maximal 2 hours.

Crypto security and Blockchain.

The use of crypto guarantees a high degree of security in itself, if the system is integer.
If crypto such as blockchain is used, we embrace the FIPS 140-2 standard for this, and have the crypto modules certified as such. This standard controls the protection of a cryptographic module within a security system. The information stored in a cryptographic module that complies with this standard is guaranteed that the confidentiality and integrity of the crypto module is guaranteed.

What is Source Code Escrow / IT Escrow

Source Code Escrow is the deposit of the source code of software with a third party escrow agent. Escrow is typically requested by a party licensing software (the licensee), to ensure maintenance of the software instead of abandonment or orphaning. The software source code is released to the licensee if the licensor files for bankruptcy or otherwise fails to maintain and update the software as promised in the software license agreement.

How we facilitate IT Escrow

On the clients request we are bound to cooperate with the facilities made available by a reliable third party for providing all requested IT Escrow Services. Our partner of choice would be: **Escrow|Ned**. Escrow is an add-on services and always provided at order by escrow agreement.

STR8LINE - THE NETHERLANDS
a brand name of Ionic Investments BV
+31 6 1991 21 88 // info@str8line.app