TINK CONNECT IT SECURITY

This document provides an overview of TinkConnect's IT security, organization and infrastructure. As an ISO 27001:2013 certified ASP/ SAAS provider, IT security is key to our operations. Enabling thousands of user actions daily requires a dependable IT security program. We ensure that all data is secured and that operations are not negatively impacted by changes, attacks or recovery procedures.

Organization

TinkConnect is ISO 27001:2013 certified with a well-established Information Security Management System (ISMS) in place. Several departments in our organization are involved in IT security and policies require the management of customer data, incident management, change management and customer relations.

Operationally, our support team is the first to act on IT security related events. Events are automatically escalated to our security team or management team as required.

Our security team's priority is optimizing current security measurements rather than dealing with daily security events. This involves employing new techniques, fine-tuning existing systems and monitoring different Internet sources for emerging threats. In addition, they provide consultancy on internal and external security questions.

We use both in-house and external training to continuously improve our level of security awareness and knowledge.

Infrastructure

As with the organization, IT security is an integral part of our system design and planning from the outset. Security starts from the bottom up and shouldn't be added as a final step in a release cycle. We believe that any change must incorporate a security component from start to finish and that our security team is consulted during the entire process.

TINK CONNECT

High availability

Any change to the platform comes with a high availability (H/A) concern. Our initial assumption is that everything should be H/A in some shape or form, unless a clear decision based on business requirements and impact analysis makes a different approach acceptable.

Standard H/A techniques used are:

- Load balancing using a farm of servers
- Clustering in an active/passive setup
- A single instance of a machine or role placed on a H/A cluster

Security domains

The hosting platform is split into several security domains. On a network level it's separated by logical networks and connected via routers and firewalls. On a functional level roles and functions are separated over different machines. This provides defence in depth with an option for granular firewall rules and permission sets, thus minimizing the impact of potential security incidents.

Filtering

Traffic flow within the network is monitored and filtered on several layers.

Firewalls are used to manage and filter both incoming and outgoing traffic as well as traffic between security domains. To do this, we use a global blacklist - updated on a daily basis - to filter malicious hosts.

Reverse and http proxies and spam filtering operating at layers 4 and 7 are employed to re-route incoming and outgoing data streams, filtering content as needed (i.e. known CVE's, brute force, viruses, etc.).

A DNS based filtering system is in place to protect users from accessing malware or other invalid content.

Antivirus is used as the last line of defence to prevent malware from being executed.

Multiple sites

Key platform components are spread over multiple sites. These include:

- User details
- Log data
- Back-up data

Encryption and VPN

Virtual private networks can be constructed to provide secure communication between client sites and the hosting platform. A fully encrypted and managed connection is used to transfer data and perform maintenance.

Where feasible, data is encrypted during transfer and at rest using established encryption algorithms.

TINK
CONNECT

Monitoring and logging

A large monitoring and logging framework manages events generated throughout the day. A list of common events and triggers are:

- User actions
- Firewall events (rejects, unusual traffic, black-lists)
- Web traffic (incoming and outgoing)
- Condition of servers, services and network
- Common vulnerabilities

Events are used to act on active issues and also for analysis and trend reporting.

Use of OTAP

TinkConnect makes extensive use of our OTAP set-up to test new functionalities and changes before deploying to production. Both software development and systems development are performed in a controlled environment. Where possible, customers are advised on using the same procedures for their own development cycles.

Back-up and continuity

Back-up is an important part of TinkConnect's infrastructure. Off-site storage is mandatory and back-up to tape is offered to clients who require longer data retention periods. We provide continuity through our organizational and technical constructions in the event of a disaster.

External cloud use

The use of external cloud solutions is limited and is primarily employed to satisfy a specific client request. Where possible, we provide our own in-house solution.

CALL TINKCONNECT!

TinkConnect provides high quality security management to your workplace and company data. We'll be delighted to meet you, learn about your needs and explain our tape back-up solution.

Call TinkConnect for an appointment on **+31 207508359**
Alternatively email your questions to info@tinkconnect.com

TINK CONNECT

ABOUT TINKCONNECT

We're here for entrepreneurs

TinkConnect is all about enterprises. We are a dedicated IT partner for large and small companies. We ensure that entrepreneurs can work and grow without having to worry about their digital back office.

IT solutions

Our package provides you with key services including working online, database management, website and application hosting and development. We also help companies migrate to the cloud. Your business will be digitalized quickly.

Personal support

Every business needs personal support with applications and their server platform. We offer a uniquely personal service. Our support desk knows exactly which applications our clients are using and how their IT environment is built.

Security first

TinkConnect's focus on security is total. With additional services including Managed Desktop, Secure Internet, Multi-Factor Authentication and Tape Back-up we improve our clients' information security.

ISO CERTIFICATION

TinkConnect is one of the few Dutch IT companies with ISO 27001 certification. Ernst & Young have performed our annual audit since 2010. This means our clients can rely on transparent processes and first-rate information security.

Amsterdam Office
Wamberg 37
1083 CW Amsterdam
The Netherlands

The Hague Office
Kneuterdijk 2
2514 EN The Hague
The Netherlands

T +31 207508359
info@tinkconnect.com
www.tinkconnect.com