Security Statement
SphinxOnline 4.17

Last update : 20/08/2019

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Phone : +33 4.50.69.82.98 - Fax : +33 4.50.69.82.78
Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

Summary

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Phone : +33 4.50.69.82.98 - Fax : +33 4.50.69.82.78
Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

1 Introduction

Sphinx company publishes and distributes solutions for surveys and data analysis since 1985.
For over 15 years, Sphinx provides hosted services to lead online surveys projects.
SphinxOnline solution is directly accessible on Internet to allow to create questionnaires, distribute surveys, hosting data and share results in interactive reporting.
Since, security and availability has become one of our main concerns.

This statement aims to list and describe all measures to meet this goal.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Phone : +33 4.50.69.82.98 - Fax : +33 4.50.69.82.78
Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

2 Infrastructure

2.1 Hosting

The servers are hosted in the OVH Datacenter, which provides physical security. The data is stored in Roubaix and Strasbourg, France.
The hosting services and infrastructures (Datacenter, servers, networks) provided by OVH are certified ISO 27001:2013.
Server management is provided by our services. Our provider does not have access to the data stored on the servers.

2.2 Network and communication protocols

The production servers are isolated in a DMZ and are protected against intrusion by a network firewall. The DMZ zone is only accessible over the TCP protocol on ports 80 and 443.
Traffic arriving on port 80 (http) are automatically redirected to port 443 (https).

OVH provides a mitigation solution that protects the infrastructure from a massive denial-of-service attack without blocking legitimate flows.

All data exchanged between the client software (Internet browser or Sphinx IQ/IQ2) and the server are encrypted using the TLS protocol.

SSL is disabled. Version 1.2 of the TLS protocol is used in priority, TLS 1.1 and lower versions can be accepted if the user's browser does not support higher versions.

Certificates are generated from 2048 bits keys and signed with the sha256 algorithm.

2.3 Systems Security

Access to the servers are restricted to IT department employees (<8 persons) and is secured through a VPN connection (IPsec or SSL with two-factor authentication tunnels)
Domain administrator, physical machine administrator and virtual machine administrator access are different. Each access is nominative.
The passwords of these administrators comply with the following policy rules and must:

- be at least 14 characters long
- have at least one number, one lowercase letter, one upper case letter, one special character
- be different from the previous 24 passwords
- be renewed every 6 months

After 5 unsuccessful access attempts, account authentication is unavailable for 60 minutes.

The passwords of the local administrators of each machine are changed to passwords of at least 22 characters with at least one digit, one lowercase, one uppercase and one special character.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Phone : +33 4.50.69.82.98 - Fax : +33 4.50.69.82.78
Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

2.4 Anti-virus protection

Antivirus administration is centralized.
Software antivirus protection is installed on all servers.
Alerts are reported in real time and protection is checked daily.

The strategies in place include, among others:

- complete analysis every week
- real-time protection
- daily update of the signature database

2.5 Criticals workstations security

Critical workstations (developers, administrators, support service,...) are password protected.
Disks are encrypted using BitLocker
Computer is automatically locked after 10 minutes of inactivity.

All workstations are protected by antivirus software.

2.6 Availability

An availability rate of 99.9% for Sphinx servers is guaranteed over 365 days.
This rate does not consider interruptions related to scheduled maintenance.
This one is held once or twice a month between 3:00 am and 4:00 am (UTC +1).
If they have to be held outside this time period, the details of the intervention will be communicated to the account owners or their administrative manager at least two weeks before.

2.7 Continuity of service

The service continuity arrangements are described in the service continuity plan.
This document is confidential but covers the following points:

- Background and infrastructure
- Diagnostic assistance and intervention triggers
- Failure scenario
- Network Connectivity Loss: Vrack, VLAN configuration,...
- Physical server hardware failure: Host, domain controller, backup server
- Failure of the virtual machine acting as a firewall or loss of its configuration

In the event of server failure, the service will be restored to another machine within a maximum of 8 hours after notification of the failure.
The maximum data loss is 24 hours.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Phone : +33 4.50.69.82.98 - Fax : +33 4.50.69.82.78
Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

The servers are currently hosted by OVH (https://www.ovh.com), so the continuity of SPHINX services is subject to the continuity of Internet access provided by OVH. In the event of interruption of this service, for any reason whatsoever, LE SPHINX DEVELOPPEMENT undertakes to do everything possible to find a new supplier.

The data is stored on disk groups in RAID 5 or Raid 50. A monitoring system alerts our teams in the event of a disk failure.

2.8 Monitoring

Applications, systems and network are monitored 24 hours a day, 7 days a week.
Remote access tests to applications from different location are carried out on a regular basis by INTERNETVISTA (www.internetvista.com).
Our teams operate from 8am to 11pm, 7 days a week in the event of an alert being sent up by the different monitoring tools.

2.9 Backup Management

The data are backed up daily and are kept for a maximum period of 6 months.
They can be retrieved on demand until 2 months after the expiration of the subscription.
These backups are encrypted using the AES algorithm (256 bits).

Backup data is replicated between the Roubaix and Strasbourg data centers.

2.10 Update Management

Operating system updates are performed within a maximum of 7 days after the patches are made available. Updates are approved manually (WSUS features).

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Phone : +33 4.50.69.82.98 - Fax : +33 4.50.69.82.78
Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

3 SphinxOnline solution

3.1 Access protection :

The security of the user accounts is ensured by login / password.
Passwords are stored on servers in a non-reversible encrypted manner (HASH PBKDF2, HMAC-SHA256, 128-bit salt, 256-bit subkey, 10000 iterations)

Passwords must meet certain minimum complexity requirements (8 alphanumeric characters and special characters) and must be changed to a minimum every 6 months.
The last 5 passwords cannot be reused.
After 5 unsuccessful access attempts, the account login is blocked for 5 minutes.

Dual factor authentication is available. This allows the user to protect access to the account with a second one-time code generated by a third-party application.
Access to surveys and / or add-ons can also be password protected.

3.2 Incident management

The technical support service is available at 04 50 69 82 98 from Monday to Thursday from 8:30 am to 12:30 pm and from 2 pm to 6 pm and Friday from 8:30 to 12:30 and from 14h to 17h (Paris time).

The response times for performing a corrective update depend on the type of anomaly:

MALFUNCTION		
Type	Définition	Correction time
Blocking	Refers to any anomaly that makes it impossible to use a feature without a workaround.	Within 8 working hours
Major	Refers to any anomaly involving degraded operation of at least one feature	Within 72 working hours
Minor	Refers to any anomaly that has a workaround, without degrading the overall operation.	Available during minor updates

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Phone : +33 4.50.69.82.98 - Fax : +33 4.50.69.82.78
Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

The correction time starts at the discovery of the problem.

VULNERABILITIES			
Impact level	Impact	Ease of exploitation	Correction time
Critical	Critical	Easy to Moderate	Within 8 working hours
	Major	Easy	
Major	Critical	Elevée	Within 72 working hours
	Major	Moderate to high	
	Significant	Easy	
Significant	Critical ou Major	difficult	Available during next minor updates
	Significant	Moderate to high	
	Minor	Easy	
Minor	Significant	Difficult	Available during minor updates
	Minor	Moderate to difficult	

3.3 Transmission security

When publishing or importing a survey from the Sphinx IQ / IQ2 software, the files exchanged between the server and the software are stored in an encrypted archive (128-bit AES algorithm).
The transmission is only done after checking the user's login/password (request encrypted in AES 256 bits).

3.4 Portability of the data

It is possible to export survey, email or SMS data in different standard formats like .csv or .xls

3.5 Traceability

Queries and connections are logged in application event logs. These logs record all the connections, recordings, modifications, navigation actions of the respondents, ... These logs are kept for a period of one year then are automatically deleted

3.6 Cookies

The SphinxOnline solution uses only technical cookies necessary for the proper functioning of the applications for the following purposes: - Security guarantee: authentication, access control, ... - Preferences: Choice of language, current working directory, display options, ... These cookies are not communicated to any third party and are not exploited for advertising or targeting purposes.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Phone : +33 4.50.69.82.98 - Fax : +33 4.50.69.82.78
Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

4 Administrative and organizational security

4.1 Vulnerabilities management

SPHINX DEVELOPPEMENT is held to an obligation of means to ensure the integrity of the network and systems against any act of external malicious or known cyber-attack.

In the event of an attempt or suspicion of breach of information security or theft of personal data. We undertake to notify the owner of the account within 8 business hours from the discovery of the problem.

Our teams monitor daily the alerts issued by CERT-FR and, when necessary, take the appropriate measures to guard against the vulnerabilities mentioned in these alerts, which may involve the application of corrective measures or the implementation of recommendations.

4.2 Control and monitoring measures

A configuration audit and intrusion tests on the solution are performed each year by an external firm specializing in computer security. In 2018, the firm Oppida was mandated; The summary of the counter-audit report conducted by Oppida in 2018 is available on request.

Any critical faults reported during these audits are corrected as soon as possible.

An internal document lists all possible improvements in terms of security. Each element of this document categorized according to several criteria (exploitability, difficulty of implementation, criticality, probability ...). A monthly review of this document is performed to update the elements with regard to the state of the art in terms of safety and to define future actions.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Phone : +33 4.50.69.82.98 - Fax : +33 4.50.69.82.78
Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34