Déclaration de sécurité

Dernière mise à jour : 05/02/2025

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Tél : 04.50.69.82.98 - Fax : 04.50.69.82.78
Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

Table des matières

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Tél : 04.50.69.82.98 - Fax : 04.50.69.82.78 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

La société Sphinx Développement édite et distribue depuis plus de 30 ans des solutions logicielles dédiées à l'enquête et l'analyse de données. Depuis maintenant plus de 20 ans, Le Sphinx Développement propose des services hébergés pour permettre à ses clients de réaliser des projets d'enquêtes en ligne en toute autonomie. Un ensemble d'applications est ainsi accessible directement via Internet pour permettre de paramétrer les questionnaires, diffuser les enquêtes, héberger l'ensemble des données collectées et partager des résultats sous forme de rapports interactifs.
Ce document a pour objectif de lister et décrire l'ensemble des mesures prises et les dispositifs mis en place pour garantir ces objectifs de disponibilité, confidentialité et d'intégrité tout en respectant les exigences réglementaires.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Tél : 04.50.69.82.98 - Fax : 04.50.69.82.78 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 Hébergement

Les serveurs sont hébergés dans les Datacenters de la société OVH qui en assure la sécurité physique. Les données sont stockées à Roubaix, Strasbourg et Gravelines en France.
La fourniture et l'exploitation des infrastructures (Datacenter, serveurs, réseaux) assurée par OVH sont certifiées ISO 27001.
L'infogérance des serveurs est assurée par nos services. Notre hébergeur n'a pas accès aux données stockées sur nos serveurs et fournit les garanties nécessaires quant à la non-intrusion d'individu dans leurs centres de données.

Localisation des datacenters :

Route de la ferme Masson, 59820 Gravelines, France
2 Rue Kellermann, 59100 Roubaix, France
140 Quai du Sartel, 59100 Roubaix, France
201 boulevard Beaurepaire, 59100 Roubaix, France
9 Rue du Bass. de l'Industrie, 67000 Strasbourg, France

2.2 Réseau et protocoles de communications

Les serveurs de productions sont isolés dans une DMZ et sont protégés contre les intrusions par un pare-feu réseau. La zone DMZ n'est accessible depuis internet que sur le protocole TCP sur les ports 80 et 443.
Les flux arrivant sur le port 80 (http) sont automatiquement redirigées vers le port 443 (https).

OVH intègre une solution de mitigation qui protège l'infrastructure d'une attaque massive en déni de service sans bloquer les flux légitimes.

Toutes les données échangées entre les logiciels clients (navigateur internet ou Sphinx IQ2/IQ3) et le serveur sont chiffrées via le protocole TLS.

Les protocoles SSL sont désactivés. La version minimale du protocole TLS utilisable est TLS 1.2.
Les certificats sont générés à partir de clés 2048bits et signés avec l'algorithme sha256.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Tél : 04.50.69.82.98 - Fax : 04.50.69.82.78 Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

2.3 Contrôle des accès systèmes

L'accès aux serveurs est réservé au personnel du service exploitation (<8 personnes) et se fait à travers d'une connexion VPN (tunnel IPsec ou SSL avec authentification à double facteur).

Les accès administrateur des domaines, administrateur de machines physiques et administrateur de machines virtuelles sont distincts. Chacun de ces accès est nominatif.

Les mots de passe de ces administrateurs respectent la politique suivante et doivent :

- comporter au moins 14 caractères dont au moins un chiffre, une minuscule, une majuscule et un caractère spécial
- être différents des 24 mots de passe précédents
- être changés tous les 6 mois

Au bout de 5 tentatives d'accès infructueuses, l'authentification au compte est impossible durant 60 minutes.

Les droits d'accès sont revus à minima semestriellement sur le principe du moindre privilège. En cas de cessation de contrat, les accès sont révoqués immédiatement.

Les mots de passe des administrateurs locaux de chaque machine sont changés pour des mots de passes distincts de 22 caractères minimum comportant au moins un chiffre, une minuscule, une majuscule et un caractère spécial.

2.4 Protection anti-virus

Une protection antivirus logicielle est installée sur tous les serveurs. L'administration de celle-ci est centralisée. Les alertes sont remontées en temps réel et la protection vérifiée quotidiennement.
Les stratégies en place incluent notamment :

- une analyse complète chaque semaine
- la protection en temps réel
- une mise à jour de la base de signature toutes les trente minutes en moyenne.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Tél : 04.50.69.82.98 - Fax : 04.50.69.82.78 Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

2.5 Sécurité des postes de travail

Les postes de travail sont protégés par mot de passe, les disques sont chiffrés (BitLocker) le verrouillage de l'ordinateur est automatique après 10 minutes d'inactivité.

Seuls les utilisateurs avec privilèges (pôle informatique) et les équipes techniques (support, produit, développement, exploitation) sont administrateurs de leur poste.

L'intégralité des postes bénéficie d'une protection anti-virus et d'un pare-feu local.

2.6 Disponibilité

Un taux de disponibilité des serveurs Sphinx est garanti à hauteur de 99.9% sur 365 jours. Ce taux ne tient pas compte des interruptions liées à des maintenances programmées.
Ces dernières ont lieu 1 à 2 fois par mois en moyenne entre 3h00 et 4h00 du matin (heure de Paris par defaut). Si elles doivent être effectuées en dehors de ce créneau horaire, les détails de l'intervention sont communiqués aux propriétaires des comptes ou au responsable de l'administration de ceux- ci dans un délai préalable de deux semaines.

2.7 Continuité des services

Les dispositifs de continuité de service sont décrits dans le plan de continuité de service.
Ce document est confidentiel mais il couvre les points suivants :

- Contexte et infrastructure
- Aide au diagnostic et seuils de déclenchement des interventions
- Scénario de panne
- La Perte de Connectivité réseau : Vrack, configuration VLAN , ...
- Défaillance matériel serveur physique : Host, contrôleur de domaine, serveur de backup
- La défaillance de la machine virtuelle remplissant le rôle de pare-feu ou la perte de la configuration de celle-ci

En cas de défaillance du serveur, le service sera rétabli sur une autre machine dans un délai maximum de 8 heures suivant la notification de la panne.
La perte de données maximale selon le scénario de panne est comprise entre 6 et 24 heures.

Les serveurs étant actuellement hébergés par la société OVH (https://www.ovh.com), la continuité des services SPHINX est donc assujettie à celle de l'accès internet fourni par OVH. En cas d'interruption de ce service, pour quelque cause que ce soit, la société LE SPHINX DEVELOPPEMENT s'engage à faire tout son possible pour trouver un nouveau fournisseur.

Les données sont stockées sur des regroupements de disques en RAID. Un système de monitoring permet d'alerter nos équipes en cas de défaillance d'un disque.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Tél : 04.50.69.82.98 - Fax : 04.50.69.82.78 Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

2.8 Surveillance

Les applications, les systèmes et le réseau sont monitorés 24h sur 24 et 7 jours sur 7. Des tests d'accès distants aux applications, à l'international sont réalisés de façon récurrente par la société INTERNETVISTA (www.internetvista.com).
Nos équipes interviennent de 8h à 23h (heure de Paris), 7 jours sur 7 en cas d'alerte remontée par les différents outils de monitoring.

2.9 Gestion des Sauvegardes

Les sauvegardes :

- quotidiennes sont conservées entre 3 et 4 mois
- complètes mensuelles sont conservées 6 mois

Ces sauvegardes sont chiffrées via l'algorithme AES (256 bits).

Les données de sauvegardes sont répliquées quotidiennement entre les infocentres de Roubaix, Strasbourg et Gravelines et sont stockées sur un VLAN différent des machines sauvegardées.

Des tests de restauration sont effectués trimestriellement.

2.10 Gestion des Mises à jour

Les mises à jour des systèmes d'exploitation sont effectuées dans un délai maximum de 7 jours après la mise à disposition des correctifs. L'approbation des mises à jour est effectuée manuellement (fonctionnalités WSUS). L'impact des mises à jour est d'abord évalué sur les environnements de test et de préproduction.

2.11 Chiffrement des données au repos

Les disques durs des serveurs sont chiffrés avec la solution BitLocker. Les clefs de chiffrement sont enregistrées dans un gestionnaire de mot de passe. L'accès à ce gestionnaire est limité aux administrateurs systèmes.

2.12 Journalisation et surveillance

L'ensembles des accès aux serveurs, une grande partie des journaux systèmes et l'intégralité des journaux de serveurs web sont envoyés en temps réel sur un système de centralisation des logs.

Des alertes sont paramétrées au niveau du SIEM pour faire remonter les évènements nécessitant le diagnostic ou l'intervention des équipes.

La rétention est d'au moins 60 jours calendaires.

2.13 Politique de restriction de la surface d'attaque

Les serveurs sont configurés pour n'exposer ou n'utiliser que les fonctionnalités, protocoles et service strictement nécessaire à l'exécution des applicatifs et des services proposés.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Tél : 04.50.69.82.98 - Fax : 04.50.69.82.78 Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

3 Sécurité des développements

3.1 Cloisonnement des environnements

Les environnements de développement, de préproduction et de production sont configurés sur des machines virtuelles et des bases de données distinctes.

Les environnements de production ne sont pas accessibles par les développeurs.

Les données utilisées pour les tests sont fictives ou anonymisées.

3.2 Formation et sensibilisation

Les équipes de développement et d'exploitation sont sensibilisées aux bonnes pratiques et au respect du TOP10 OWASP

3.3 Conception et spécification

Les fonctionnalités sont pensées afin de :

- respecter le principe de "sécurité par défaut"
- prévenir les utilisateurs et utilisatrices en amont d'une action ayant un impact sur la sécurité des données.
- proposer un niveau de mots de passe fort

3.4 Bonnes pratiques

Les entrées extérieures (valeurs textuelles, données externes ou librairie tierces) sont systématiquement vérifiées et filtrées si nécessaires. Un filtrage en sortie est effectué pour les applications qui desservent les contenus aux utilisateurs.

Une inspection profonde est effectuée de manière systématique sur les fichiers uploadés.

Les techniques de développement incluent plusieurs mécanismes pour se protéger des injections SQL :

- la validation de données en entrée
- requête SQL construite de façon paramétrique
- utilisation d'un ORM

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Tél : 04.50.69.82.98 - Fax : 04.50.69.82.78 Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

Une attention particulière est apportée :

- au blocage des énumérations
- à l'enregistrement et lecture des fichiers
- aux injection cross-site scripting (XSS)
- à la protection des cookies

3.5 Gestion des évolutions

Un contrôle du code source est mis en place. Il permet la gestion de branche, des nouvelles versions et le suivi des correctifs déployés. Les notes de mise à jour se font sur plusieurs niveaux.

Le serveur de contrôle de code source est internalisé et administré par les équipes du pole exploitation. Il est accessible uniquement par VPN.

3.6 Surveillance des dépendances

Un système d'alerte sur les versions des librairies utilisées dans nos applications est mis en place : les versions obsolètes ou touchées par des vulnérabilités sont surveillées. L'intégration des nouvelles versions est réalisée au plus tôt en accord avec la continuité fonctionnelle des applications et des risques.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Tél : 04.50.69.82.98 - Fax : 04.50.69.82.78 Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

4 Applications Saas

4.1 Authentification et protection des accès

La sécurité des comptes utilisateurs est assurée par login/mot de passe.

Les utilisateurs doivent définir leur mot de passe dès leur première connexion.

Les mots de passe sont stockés sur les serveurs de manière chiffrée non réversible (HASH PBKDF2 HMAC-SHA256, 128-bit salt, 256-bit subkey, 10000 itérations).
Les mots de passe doivent respecter certaines contraintes de complexité minimales (12 caractères alphanumériques et caractères spéciaux) et doivent être changés à minima tous les 6 mois.
Les 5 derniers mots de passe ne peuvent pas être réutilisés.
Après 5 tentatives infructueuses d'accès, la connexion au compte est bloquée pendant 5 minutes.

Une authentification à double facteur est disponible. Celle-ci permet à l'utilisateur de protéger l'accès au compte avec un deuxième code à usage unique généré par une application tierce ou une clé personnelle.

L'accès aux enquêtes et/ou modules complémentaires peut également être protégé par mot de passe. Cette protection est active par défaut.

Par défaut les sessions sont limitées dans le temps selon les durées suivantes :

- 8 heures glissantes pour les profils utilisateurs
- 45 minutes non glissantes pour les profils administrateurs

Les administrateurs de la solution ont la possibilité de se connecter sur un compte utilisateur. Ce type d'accès n'est autorisé qu'en cas de demande d'assistance ou suspicion d'atteinte à la confidentialité ou l'intégrité des données. La durée de validité de ce type d'accès est fixée à 20 minutes non glissantes.

Au-delà de ces délais, les jetons utilisés sont révoqués et ne peuvent plus être réutilisés.

Les cookies de session sont révoqués à la déconnexion de l'utilisateur.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Tél : 04.50.69.82.98 - Fax : 04.50.69.82.78 Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

4.2 Gestion des Incidents

Le service de support technique est accessible au 04 50 69 82 98 du lundi au jeudi de 8h30 à 12h30 et de 14h à 18h et le vendredi de 8h30 à 12h30 et de 14h à 17h (heure de Paris).

Les délais de correction sont indicatifs et courent à compter de la notification du problème et dépendent du type d'anomalie.

ANOMALIE FONCTIONNELLE		
Type	Définition	Délais de correction
Bloquante	Désigne toute anomalie rendant impossible l'utilisation d'une fonctionnalité, sans solution de contournement.	Sous 8 Heures Ouvrées
Majeure	Désigne toute anomalie impliquant un fonctionnement en mode dégradé d'au moins une fonctionnalité.	Sous 72 Heures Ouvrées
Mineure	Désigne toute anomalie disposant d'une solution de contournement, sans dégradation du fonctionnement global.	Mise à disposition lors des mises-à-jour mineures

FAILLE DE SECURITE			
Niveau de risque	Impact	Facilité d'exploitation	Délais de correction
Critique	Critique	Facile à modéré	Sous 8 Heures Ouvrées
	Majeur	Facile	
Majeur	Critique	Elevée	Sous 72 Heures Ouvrées
	Majeur	Modérée à élevée	
	Important	Facile	
Important	Critique ou Majeur	Difficile	Mise à disposition au plus tard lors de la prochaine mise-à-jour mineure
	Important	Modérée à élevée	
	Mineur	Facile	
Mineur	Important	Difficile	Mise à disposition au plus tard lors des mises-à-jour mineures
	Mineur	Modérée à difficile	

4.3 Sécurité des échanges

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Tél : 04.50.69.82.98 - Fax : 04.50.69.82.78 Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

Lors de la publication ou de l'importation d'une enquête à partir du logiciel client Sphinx IQ3, les fichiers échangés entre le serveur et le logiciel sont stockés dans une archive chiffrée (algorithme AES 128 bits). L'échange de fichiers n'est effectué qu'après vérification du couple login/mot de passe de l'utilisateur (requête chiffrée en AES 256 bits).

4.4 Réversibilité et portabilité des données

Il est possible d'exporter les données d'enquêtes, campagnes d'emailing ou SMS dans différents formats standards comme .csv ou .xlsx.

Les comptes clients ainsi que les données associées sont supprimées des serveurs de production deux mois après l'expiration de l'abonnement ou la fin de la prestation.
Les clients peuvent prendre contact avec le support technique pour la restitution ou la destruction des données avant la fin de ces deux mois.
Un PV de destruction peut être fourni sur demande.

4.5 Traçabilité et journalisation

Les requêtes et les connexions sont consignées dans des journaux d'événements applicatifs. Ces journaux enregistrent toutes les connexions, enregistrements, modifications, actions de navigation des répondants…
Ces journaux sont sauvegardés et conservés pendant une période d'un an puis sont automatiquement supprimés.

4.6 Cookies

La solution SphinxOnline utilise uniquement des cookies techniques nécessaires au bon fonctionnement des applications pour les objectifs suivants :

- Garantie de sécurité : authentification, contrôle d'accès, …
- Préférences : Choix de langue, répertoire de travail courant, options d'affichages, …

Ces cookies ne sont communiqués à aucun tiers et ne font pas l'objet d'une exploitation à des fins publicitaires ou de ciblage.

4.7 Filtrage applicatif

Un pare-feu applicatif (WAF) assure un filtrage supplémentaire en amont des solutions Saas
Cette solution assure le rôle de reverse-proxy ainsi que plusieurs niveaux de filtrage :

- réputation par IP
- détection comportementale et anti brut force
- analyse en profondeur des requêtes pour détecter des attaques connues ou génériques, tentative cross-site scripting, …

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Tél : 04.50.69.82.98 - Fax : 04.50.69.82.78 Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

5 Sécurité administrative et organisationnelle

5.1 Gestion des failles de sécurité

La société SPHINX DEVELOPPEMENT est tenue à une obligation de moyen pour assurer l'intégrité du réseau et des systèmes contre tout acte de malveillance extérieur ou toute attaque informatique connue.

En cas de tentative, ou de suspicion d'atteinte à la sécurité de l'information ou de vol de données personnelles. Nous nous engageons à avertir le propriétaire du compte dans les 8 Heures Ouvrées à compter de la découverte du problème.

Nos équipes suivent quotidiennement les alertes émises par le CERT-FR et, lorsque c'est nécessaire, prennent les mesures adéquates pour se prémunir des vulnérabilités évoquées dans ces alertes, ce qui peut impliquer l'application de correctifs ou la mise en place des recommandations.

5.2 Gestion des incidents de sécurité

Lors d'un incident de sécurité, le DPO (dpo@lesphinx.eu) et le RSSI doivent être informés dès la prise de connaissance du problème.

Dans les deux heures suivant la phase de diagnostic initiale, une première qualification de l'incident est réalisée afin de prendre les mesures palliatives adéquates (interruption de service, limitation des accès…). Si nécessaire, le DPO et/ou le RSSI acterons un passage en situation de gestion de crise afin de mobiliser toutes les ressources disponibles.

Selon l'origine du problème, des solutions de corrections ou de mitigations devront être proposées et arbitrées en comité de sécurité adapté, incluant à minima un membre par service concerné. Les mesures prises pourront inclure la modification d'applications du système, du durcissement système et réseaux, l'application de correctifs fournisseurs...

Les clients impactés seront informés dans un délai, aussi court que possible, ne dépassant pas 8h ouvrées à compter de la prise de connaissance du problème. Une communication partielle est envisageable en cas de diagnostic incomplet, à condition de le mentionner et de faire des communications ultérieures. Les contacts privilégiés seront ceux inclus dans les échanges antérieurs concernant l'incident ou, à défaut, les titulaires des comptes ou responsables de projet identifiés dans l'ERP.

La rédaction et la communication d'un « post mortem » est faite pour les incidents ayant un impact stratégique ou critique.

En cas d'incident, les clients seront avertis sur la page de connexion Sphinx Online. Pour les incidents majeurs, les titulaires de comptes concernés pourront également être avertis par email.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Tél : 04.50.69.82.98 - Fax : 04.50.69.82.78 Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

5.3 Mesures de contrôles et de suivi

Un audit de configuration et des tests d'intrusion sur la solution sont réalisés chaque année par un cabinet externe spécialisé dans la sécurité informatique. La synthèse du dernier rapport de contre audit est disponible sur demande.

Les éventuelles failles critiques remontées lors de ces audits sont corrigées dans les plus brefs délais.

Un document interne recense toutes les failles connues, les améliorations envisageables et les évolutions possibles en termes de sécurité.
Les informations sont issues de :

- Bulletin de sécurité (fournisseurs, CERT-FR, ANSSI, …)
- Remontées et besoin clients
- Synthèse d'audit
- Problématiques liées aux évolutions logicielles et/ou matérielles
- …

Chaque élément de ce document catégorisé en fonction de plusieurs critères (exploitabilité, difficulté de mise en œuvre, criticité, probabilité, …). Une révision mensuelle de ce document est effectuée pour mettre à jour les éléments au regard de l'état de l'art en matière de sécurité et pour prioriser et définir les actions à venir.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Tél : 04.50.69.82.98 - Fax : 04.50.69.82.78 Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34