Plan Assurance Securite

V1.0

Table des matières

1 PRÉSENTATION GÉNÉRALE

1.1 Objet

Ce document décrit le contenu du Plan Assurance Sécurité de l'ACSIE pour son application « ESO », acronyme de « E-Social Office ». Cette application est à destination des assistantes sociales.

Ce document ainsi que d'autres documents d'assistance, des informations de maintenance et des mises à jour de l'application par les services de l'ACSIE sont disponibles via le site internet dédié "download.eso-online.fr".

1.2 Périmètre

Il couvre les fonctionnalités relatives à la gestion des dossiers sociaux des salariés d'une entreprise par une assistante sociale.

Ce dispositif permet de proposer aux assistantes sociales les fonctionnalités :

- Gestion de fiche de personnel avec informations administratives
- Gestion de dossier social de personnel avec informations de suivi
- Gestion d'outils liés aux points ci-dessus (Carnet d'adresses, Statistiques, etc.)

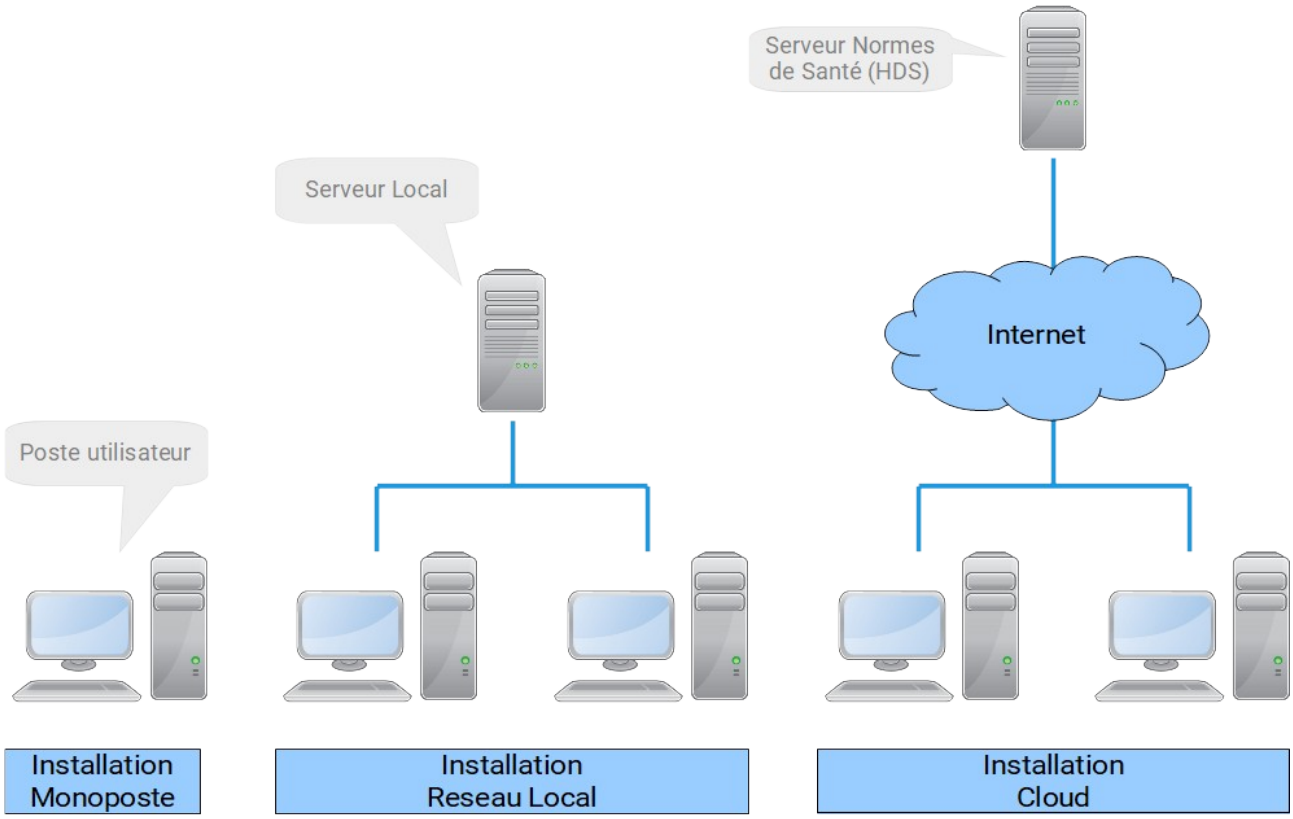
Certaines fonctionnalités non critiques (fiche administrative, statistiques, carnet d'adresses, installation de module) pourront être accessibles à du personnel non social (secrétaire, administrateur informatique, etc.) selon des réglages spécifiques.

2 ARCHITECTURE TECHNIQUE GÉNÉRALE

Trois types d'installation sont possibles :

- Installation monoposte : le poste de l'utilisateur héberge l'application.
- Installation Réseau local : un serveur héberge localement l'application, le ou les postes utilisateurs se connectent à ce serveur pour utiliser l'application.
- Installation Cloud : Le ou les postes utilisateurs se connectent à un serveur Cloud sécurisé via internet.

Le schéma suivant illustre ces trois cas sans faire apparaître les éléments complexes (pare-feu, routeurs, etc.) qui ne sont pas traités dans ce document.



3 ÉTAT DES LIEUX (MODE SAAS)

3.1 Description des entreprises

Voici une présentation des acteurs de l'application :

Entreprise	Rôle
ACSIE	Éditeur du logiciel ESO et entreprise de service social en entreprise
ALGOLYS	Entreprise de création et de maintenance de logiciels sur mesure (Sécurité des locaux, accès avec Badge et gardiennage)
IBM CLOUD	Hébergeur HDS (sécurité HDS)

3.2 Personnel chargé des interventions

Voici l'organigramme des personnes susceptibles d'intervenir sur l'application :

Prénom et nom	Entreprise	Relation clientèle	chef de projet	Administrateur Systèmes et réseaux	développeur	test
Sandrine Bugaud	ACSIE	X	X (product owner)			X
Fabien Boulling	ALGOLYS	X	X (polyvalent)	X	X	X
Fanny Bertrand	ALGOLYS	X	X (scrum master)	X	X	X
Fabrice Marchand	ALGOLYS			X		
Mathilde	ALGOLYS				X	X

Vollet						
Alban Rouault	ALGOLYS				X	X
Victor Vaizand	ALGOLYS				X	X

3.3 Règles de protection du Système d'Information

Voici les règles générales de protection du SI :

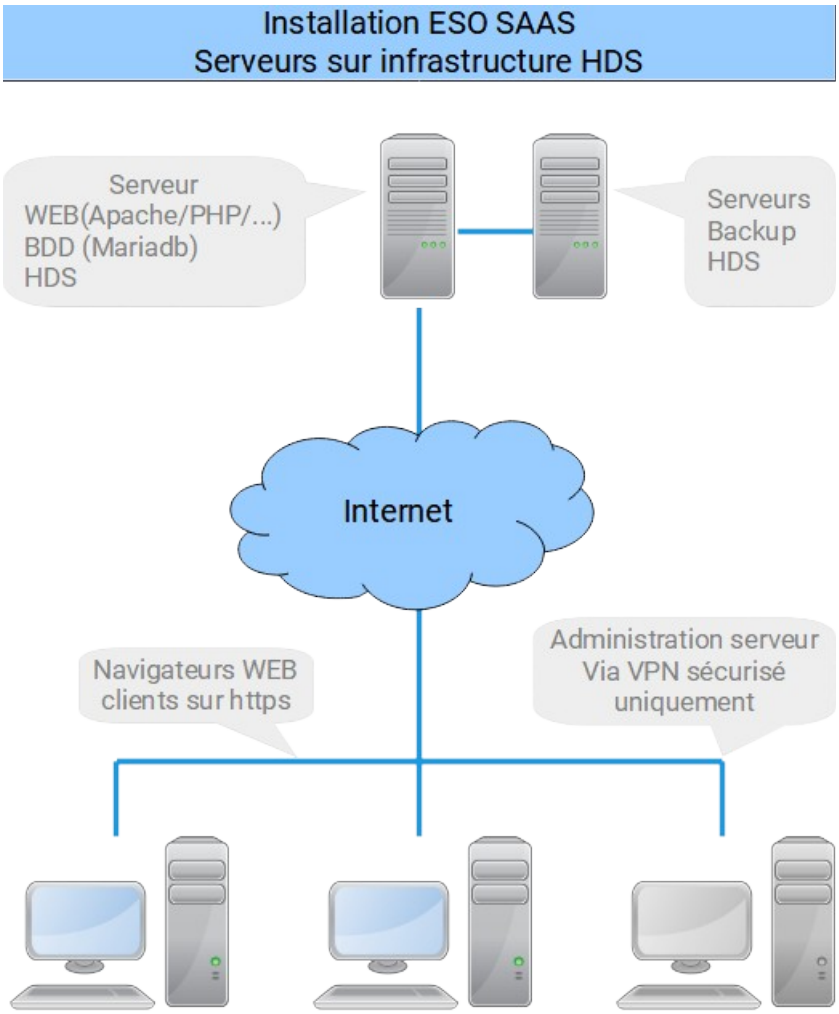
Prestation	Statut
Authentifications	Fortes avec gestionnaire de mot de passe (plus de 8 caractères avec Majuscule, minuscule, chiffre et caractère spéciaux.
	Mots de passe d'accès au Si avec hash SHA512.
	Principes de Privacy by design
	Mise à jour habituellement mensuelle. Vulnérabilité majeure bloquante : prise en compte immédiate à la communication du blocage et début de la résolution. Vulnérabilité majeure non bloquante : prise en compte sous 1 jour en général. Mise en application de la correction : Variable selon la vulnérabilité.
	documenter et maintenir à jour une cartographie des couches techniques, fonctionnelles:Voir Dossier d'architecture Technique (DAT)
	Toute personne travaillant sur le système d'information dispose d'un compte personnel, incessible et non définitif. Les comptes génériques sont interdits.
	Attribution aux comptes techniques que des accès strictement nécessaire pour répondre à l'exercice du besoin.
	Comptes par défaut modifiés
	Autorité de confiance reconnue pour la délivrance de certificats : letsencrypt
Accès aux machines	Accès aux machines physiques de développement et de maintenance sécurisés et contrôlés : - Clés - Badges - Personnel de sécurité - Équipe de maintenance avec intervention dans l'heure - etc. Accès aux serveurs protégés via règles hds.
Backup	IBM Cloud Backup (HDS)
	Avant chaque utilisation de supports amovibles, analyse de contenu, notamment à la recherche de code malveillant via déclenchement automatique de l'antivirus (ESET)

	Cryptage des disques des postes de travail
	Anonymisation possible, Purge possible
	Pas de sous traitant extra-européen

3.4 Architecture générale de la plateforme

Mode SAAS : Mise à disposition d'une plateforme WEB dédiée hébergée sur des serveurs HDS (IBM PARIS). Le client utilise sont navigateur internet conformément au Dossier d'Architecture Technique qui contient un schéma représentatif et des spécifications techniques. Données personnelles traitées de type social à caractère de sécurisation équivalent au type santé.

Sous traitance informatique à SARL ALGOLYS qui intervient via un VPN Privatif IBM Cloud sur les serveurs HDS IBM Cloud. Comptes personnalisés et backup dans l'infrastructure toujours HDS.



3.5 Accès logiques à la plateforme

identification et authentification, mise en veille, déconnexion automatique, gestion des droits, traçabilité...

4 REPRISE APRÈS SINISTRE (MODE SAAS)

4.1 Dispositions

Dispositions prises pour assurer la continuité de l'activité après sinistre ou incident majeur :

Dispositions	Détails
Gestion de ticket incident dans plateforme privative. Non suppression de l'historique des tickets	
Le plan de Continuité informatique repose sur la solution d'hébergement HDS.	

4.2 Assurances et contrôles de la sécurité

Dispositions prises pour assurer les contrôles de sécurité :

Dispositions	Détails
EX-01	Révision permanente basée sur la mise en application des recommandations du guide de l'hygiène informatique de l'ANSI et du guide des recommandations de mise en œuvre de site web de l'ANSI
EX-02	Gestion via système de tickets internes. L'appréciation des risques est couverte par les retours clients, les audits clients, le suivi des documents de l'ANSII décrits plus haut, les notifications de l'ANSII cert.ssi.gouv.fr sous forme d'alertes, de menaces, d'avis, d'indicateurs et de recommandations. Ces éléments de sécurité sont intégrés selon un ordre de priorité à notre chaîne de gestion (A faire, en cours, en test, terminé) et conservés pour archivage.

EX-03	Hébergement type HDS incluent les contrôles matériels. Contrôles logiciels basés sur audits client periodiques.
EX-04	Une clause est intégrée au dossier RGPD, contenant la liste des droits des collaborateurs sur les services à réviser (serveurs, dépôts, outils collaboratifs, etc.). Une tâche annuelle est programmée automatiquement pour réviser cette clause.