



# Plan d'Assurance Sécurité

Entr'ouvert

26 juin 2026

## Table des matières

<b>1</b>	<b>Historique</b>	<b>2</b>
<b>2</b>	<b>Objet du document</b>	<b>2</b>
<b>3</b>	<b>Documents de référence</b>	<b>2</b>
<b>4</b>	<b>Description du système externalisé</b>	<b>3</b>
<b>5</b>	<b>Rappel des exigences</b>	<b>3</b>
5.1	Organisation . . . . .	3
<b>6</b>	<b>Procédure d'évolution du PAS</b>	<b>4</b>
<b>7</b>	<b>Applicabilité du PAS</b>	<b>5</b>
<b>8</b>	<b>Mesures de sécurité</b>	<b>5</b>
8.1	Authentification et gestion des droits . . . . .	5
8.2	Imputabilité, traçabilité . . . . .	7
8.3	Mises à jour, correctifs de sécurité . . . . .	8
8.4	Gestion des incidents de sécurité . . . . .	8
8.5	Protection contre les logiciels malveillants . . . . .	9
8.6	Sauvegardes et restaurations . . . . .	9
8.7	Supports de données et équipements sensibles . . . . .	10

8.8	Intervention des sociétés de maintenance ou de support . . . . .	10
8.9	Accès distants au système d'information de nos . . . . .	10
8.10	Architecture de sécurité . . . . .	10
8.10.1	Contrôle et filtrage des flux . . . . .	10
8.10.2	Confidentialité et intégrité des flux* . . . . .	11
8.10.3	Environnements . . . . .	11
8.11	Localisation des données . . . . .	11
8.12	Continuité d'activité . . . . .	11
8.13	Développement et sécurité . . . . .	12
8.14	Appréciation des risques . . . . .	13
<b>9</b>	<b>Matrice de couverture des exigences de sécurité</b>	<b>13</b>
<b>10</b>	<b>Documentation de suivi</b>	<b>14</b>

## 1 Historique

Quand	Quoi	Qui
2026-06-26 18:17:24 +0200	apply pre-commit-pandoc (#119175)	Thomas NOËL (tnoel@entrouvert.com)
2026-06-23 16:36:34 +0200	add lang in yaml/md	Thomas NOËL (tnoel@entrouvert.com)
2026-06-23 16:23:39 +0200	add plan-assurance-securite first draft	Thomas NOËL (tnoel@entrouvert.com)

## 2 Objet du document

Le plan d'assurance sécurité précise les dispositions prises par Entr'ouvert, sur le périmètre de ses prestations, pour répondre aux clauses de sécurité.

## 3 Documents de référence

- Le contrat « Hébergement, développement et prestations associées portant sur la plateforme libre de gestion de la relation usagers « Publik »
- Le cahier des clauses techniques particulières y afférant

## 4 Description du système externalisé

Publik est une plate-forme libre et modulaire, destinée aux citoyens et aux services de l'administration publique pour simplifier leurs interactions. 10

La solution se compose de trois modules interconnectés :

- Module citoyens, le front-office : pour améliorer le service aux administrés.
- Module métier, le back-office : pour simplifier le travail des agents.
- Module paramétrage : pour le paramétrage, l'ouverture et l'interconnexion des données. 15

## 5 Rappel des exigences

Rappel des exigences en termes de sécurité de la plate-forme SaaS Publik :

**Confidentialité des données:** Les données traitées dans le cadre de la plateforme Publik contiennent des données Personnelles dépendant du RGPD. À ce titre Entr'ouvert met en place des technologies respectant les normes en vigueur et les bonnes pratiques en matière d'architectures et développements de systèmes informatiques sécurisés. 20

**Intégrité des données:** La plate-forme Publik met en relation des citoyens. De ce fait, la perte de données est problématique, on ne peut pas demander à ces citoyens de re-soumettre leurs demandes, car on ne sait pas qui a pu effectuer une démarche sur la plate-forme. C'est pour cela qu'Entr'ouvert privilégie l'intégrité des données et met en place plusieurs systèmes de sécurisation et de redondances de celles-ci. 25

**Disponibilité des données:** La plate-forme Publik possède une architecture redondée qui lui permet de faire face à plusieurs pannes matérielles ou logiciel. De plus celle-ci est configurée pour avoir assez de puissance pour pouvoir tourner avec la moitié de sa puissance nominale. Des tests de fonctionnement en mode dégradé et de bascule sont réalisés annuellement. 30

### 5.1 Organisation

Entr'ouvert s'engage à mettre en œuvre les mesures de sécurité visant apporter une protection suffisante des données. Ces mesures portent à la fois sur les données à caractère personnel confiées et sur les mesures générales de sécurité du système. 35

Entr'ouvert s'engage au respect des standards de développement et de sécurité, pour des solutions opérationnelles et pleinement interopérables.

Entr'ouvert désignera un chef de projet technique (CPT) chargé de la mise en œuvre du plan et des incidents de sécurité. Un chef de projet fonctionnel (CPF) personne ressource auprès du conseil départemental et chargé de l'organisation des comités de suivi. Un comité de suivi de la sécurité sera organisé chaque année par le CPF sur demande de l'une ou l'autre des parties. CPF et CPT assisteront aux comités de suivi.

40

Des audits pourront être commandés par nos . Entr'ouvert s'engage à fournir les informations nécessaires en vue de leur réalisation optimale. Les interventions éventuelles d'Entr'ouvert seront facturées au prorata du temps passé.

45

Le suivi de chaque incident de sécurité est centralisé via l'outil de gestion de ticket d'Entrouvert, Redmine, à l'aide d'un ticket dans l'espace dédié au client et éventuellement de tickets techniques dans les projets de développement logiciel.

Entr'ouvert reconnaît être tenu à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité et de mise à l'état de l'art. En particulier il s'engage à informer ses des risques d'une opération envisagée, des incidents éventuels ou potentiels, et de la mise en œuvre éventuelle d'actions correctives ou de prévention.

50

Entr'ouvert fournira la liste des administrateurs techniques habilités à se connecter aux machines. Entr'ouvert externalise la gestion des machines physiques, son sous-traitant est certifié ISO/CEI 27001. Les ressources liées au fonctionnement du service sont surveillées en continu.

55

Entr'ouvert forme ses travailleurs aux questions de sécurité et de confidentialités. Tous les travailleurs d'Entr'ouvert ont signé un avenant spécifique RGPD concernant le traitement des Données Personnelles

60

## 6 Procédure d'évolution du PAS

Entr'ouvert est responsable de la rédaction du PAS initial et de ses évolutions pour répondre aux clauses de sécurité du donneur d'ordres pendant toute la durée du contrat.

Une révision du Plan d'Assurance Sécurité pourra être réalisée en cas d'évolution du périmètre de l'opération, de l'environnement du S.I, ou des exigences de la maîtrise d'ouvrage, après accord de la maîtrise d'œuvre. Cette révision sera réalisée par le responsable sécurité désigné par Entr'ouvert sous forme de proposition de modification. Si cette modification est acceptée, le PAS est révisé, validé, puis diffusée à l'ensemble des acteurs pour application.

65

## 7 Applicabilité du PAS

70

Le Plan d'Assurance Sécurité est applicable à l'ensemble des acteurs du projet.

Un acteur du projet qui n'est pas à même de remplir l'ensemble des clauses du PAS devra effectuer une demande de dérogation auprès d'Entr'ouvert.

Un acteur du projet qui identifie un non-respect du PAS dans ses procédures et mesures doit en référer immédiatement Entr'ouvert.

75

## 8 Mesures de sécurité

### 8.1 Authentification et gestion des droits

Pour chaque interface d'accès au système, (Interface Homme-Machine, interface entre applications) le titulaire doit fournir une documentation précisant :

Mécanismes d'authentification mis en œuvre (protocoles, algorithmes de hachage et de chiffrement utilisés).

80

Les mécanismes d'authentification supportés sont :

- Authentification par mot de passe
- Fournisseur d'identité OpenID Connect
- Fournisseur d'identité SAML 2.0
- FranceConnect (OpenID Connect)

85

Les seuls rôles d'administration par défaut du fournisseur d'identités sont :

- Gestionnaire des rôles,
- Gestionnaire des collectivités (au sens unité organisationnelle — OU),
- Gestionnaire des usagers,
- Gestionnaire des services (i.e. des briques applicatives Publik)
- Additionnellement, chaque rôle applicatif se voit attribuer un rôle d'administration pour usage en interne du fournisseur d'identités authentic2.
- Les moyens d'authentification associés aux interfaces doivent être interopérables tant au niveau des applications des (par exemple navigateurs web, SSO Active Directory, authentification LDAP, ...) que des systèmes d'exploitation.

90

95

- Les raccordements à un Active Directory/Kerberos ou à un LDAP convenablement configurés sont supportés par Publik.
- La gestion des habilitations se fait à l'aide des rôles dans Publik (Role-based access control — RBAC). Ceux-ci sont entièrement paramétrables.

100

**Liste des dispositifs :**

- Verrouillage de la session utilisateur après une période d'inactivité. Par défaut, Publik utilise le délai standard d'expiration de la session tel que défini par le cadre web Django, qui est de deux semaines. En revanche, si le contexte de déploiement de Publik l'exige, ce délai peut-être paramétré à une valeur différente des deux semaines par défaut.
- Il est aussi possible d'activer un temps d'attente exponentiel après chaque tentative d'authentification infructueuse pour se protéger des attaques sur mot de passe par force brute.
- L'utilisateur peut à tout moment choisir de changer son mot de passe, via un formulaire dédié sur la page de gestion de son compte Publik.
- Possibilité d'affecter à un utilisateur un mot de passe temporaire devant être changé à la prochaine connexion.
- Paramétrage des droits des utilisateurs au travers de rôles en respectant le principe du moindre privilège. Ce paramétrage est directement supporté dans Publik, dû à la prise en charge du modèle de contrôle d'accès basé sur les rôles (RBAC).
- Gestion de profils utilisateurs et de profils administrateurs (fonctionnels et techniques) : la désignation des administrateurs fonctionnels et techniques parmi les utilisateurs de la plateforme Publik se fait au travers des rôles.
- Les comptes inactifs sont supprimés automatiquement au bout de deux ans. Un mail est envoyé un mois avant la suppression effective du compte. Ces deux valeurs sont paramétrables dans Publik.

105

110

115

120

**Dispositifs de contrôles :**

- La liste des permissions d'un usager peut être reconstruite à partir des rôles qu'il possède – directement, ou non (par héritage).
- Une procédure pour désactiver les comptes inactifs, inutilisés ou à bloquer est paramétrable dans le fournisseur d'identités Authentic de Publik. Les délais d'alerte à l'utilisateur de son inactivité et de désactivation du compte sont paramétrables.

125

**Procédure de traçabilité**

Les mots de passe doivent respecter l'état de l'art, par exemple la délibération

130

n°2022-100 du 21 juillet 2022 portant adoption d'une recommandation relative aux mots de passe. A minima, ils devront comporter 12 caractères avec 3 types de caractères différents. La politique de choix des mots de passe est configurable dans Publik (longueur minimale, catégories de caractères à inclure). Par défaut, les mots de passe doivent contenir au moins 12 caractères, dont au moins une majuscule, une minuscule et un caractère spécial. 135

## 8.2 Imputabilité, traçabilité

Chaque utilisateur doit posséder un identifiant dont il a la responsabilité. Cet identifiant est personnel et permet de garantir l'identité du porteur.

L'utilisation d'un même compte par plusieurs personnes n'est pas autorisée sauf si une contrainte le justifie. 140

Les comptes des usagers et des agents dans Publik sont nominatifs. Ils n'ont en aucun cas vocation à être partagés.

Pour la traçabilité, les informations suivantes sont enregistrées :

- Entrée en session d'un utilisateur : date, heure, identifiant de l'utilisateur et du terminal, réussite ou échec de la tentative, les connexions et déconnexions des usagers sont logguées par le serveur Web, i.e. nginx. 145
- Actions qui tentent d'exercer des droits d'accès à un objet soumis à l'administration des droits : date, heure, identité de l'utilisateur, nom de l'objet, type de la tentative d'accès, réussite ou échec de la tentative, la journalisation de l'ensemble des actions dans Publik est accessible. Par souci de lisibilité, un même type d'accès n'est enregistré qu'une fois par heure. 150
- Création/suppression d'un objet soumis à l'administration des droits : date, heure, identifiant de l'utilisateur, nom de l'objet, type de l'action.
- Actions d'utilisateurs autorisés affectant la sécurité de la cible : date, heure, identité de l'utilisateur, type de l'action, nom de l'objet sur lequel porte l'action. 155

Les traces sont conservées pendant la période légale relative aux données enregistrées ou, à défaut de valeur plus spécifique, pendant une période d'une année. Une fois cette période passée, si les logs doivent être conservés pour des raisons techniques ceux-ci sont anonymisés conformément aux recommandations de l'ANSSI. 160

### 8.3 Mises à jour, correctifs de sécurité

Les évolutions fonctionnelles ou techniques ne doivent pas remettre en cause le respect des mesures de sécurité. Si un contournement provisoire nécessite la désactivation d'une fonctionnalité indispensable au système, Entr'ouvert s'engage à proposer des mesures permettant d'éviter l'exploitation de la vulnérabilité dans un délai inférieur à 15 jours. 165

Le traitement des alertes de sécurité mineures doit intervenir durant les périodes de maintenance hebdomadaires ou mensuelles dans un délai de 30 jours.

Les passages de correctifs doivent être précédés d'une sauvegarde spécifique du système et des données qu'il contient, ainsi que de tests sur un environnement de pré production. 170

Entr'ouvert fournit des notes de mise à jour systématiquement. Outre les apports fonctionnels, les notes de mise à jour contiennent notamment les correctifs de sécurité – <https://doc-publik.entrouvert.com/notes-de-mises-a-jour/>

En cas d'alerte donnée par les équipes d'Entr'ouvert, les opérations de mise en sécurité seront notifiées en amont, sur la liste courriel du projet. 175

Le support Entr'ouvert est disponible aux heures ouvrées (9h30-12h30 et 14h00-18h00) les jours ouvrés, joignable sur la plateforme de gestion de ticket.

### 8.4 Gestion des incidents de sécurité

Une procédure de gestion des incidents de sécurité est formalisée.

Tout incident de sécurité (anomalie, irrégularité, malveillance, fraude, vulnérabilités, vol de données, comportement anormal) sera signalé auprès de nos dans les meilleurs délais et au maximum dans les 12 heures. 180

Les canaux de communication des incidents sont:

- dev.entrouvert.org
- status.entrouvert.org
- les mailings listes, particulièrement la mailling liste de gestion des incidents. 185

Tout incident de sécurité détecté fera l'objet d'une analyse et une qualification sera réalisée sur les impacts potentiels en fonction de la criticité des ressources impactées, de l'étendue du périmètre, de la durée de l'incident. De façon plus générale, nous procédons à des post-mortems, détaillant l'origine de la panne et les corrections apportées. Ces post-mortems sont archivés et une communication est faite a tous les 190

clients concernés en fin d'analyse.

## 8.5 Protection contre les logiciels malveillants

La politique de protection comporte notamment les éléments suivants :

- L'usage de clés SSH nominatives. 195
- Utilisation exclusive du système d'exploitation Debian avec dépôts de paquets officiels, que ce soient sur les serveurs ou les postes de travail des membres de l'équipe
- Le module de noyau de sécurité AppArmor.
- De façon plus générale, l'usage systématique d'outils libres, dont le code est donc auditable. 200
- Le système d'identification de l'expéditeur, DKIM, est activé sur le serveur de messagerie. DKIM permet de s'assurer qu'il s'agit bien du détenteur du domaine qui envoie des courriels en son nom.
- Un système d'alerte sur les opérations jugées suspectes est en place sur le serveur. 205
- L'équipe technique effectue une veille des vulnérabilités en étant abonnée aux alertes de sécurité de l'ANSSI (<https://www.cert.ssi.gouv.fr/>) et des logiciels utilisés sur notre plate-forme Publik.

### Cas des pare-feu applicatifs

Les pare-feux applicatifs sont utilisés pour sécuriser une application web ou accessible en réseau des vulnérabilités connues et non corrigés de l'applicatif. 210

Nous utilisons ce type de pare-feu dans une optique de surveillance et de détection rapide de vulnérabilités potentielles, afin de les corriger au plus vite. Nous mettons en place une procédure de « hotfix » en cas d'alerte de sécurité.

Nous utilisons également des pare-feu réseau et des mécanismes de blocage en cas de saturation du SaaS. 215

## 8.6 Sauvegardes et restaurations

Entr'ouvert gère la sauvegarde de toutes ses installations, les sauvegardes sont quotidiennes (nocturnes) et conservées :

- quotidiennement pendant une semaine, 220
- hebdomadaires sur 1 mois,
- mensuelles sur 4 mois.

En plus des sauvegardes complètes à chaud des systèmes, un archivage des transactions des bases de données est réalisé, cela permet de rejouer les modifications de données et de récupérer des données à la minute. Les restaurations sont testées régulièrement. 225

Entr'ouvert dispose d'une procédure de restauration simple, que ce soit une restauration partielle « sur site » ou totale sur une nouvelle instance.

Les sauvegardes sont situées sur un autre site géographique que le site de production. Tous les flux lors des opérations de sauvegarde sont chiffrés, les disques stockant les sauvegardes ne le sont pas. 230

## 8.7 Supports de données et équipements sensibles

La gestion des supports est opérée par notre hébergeur OVH. Nous ne possédons pas les machines, mais les louons directement à OVH.

## 8.8 Intervention des sociétés de maintenance ou de support

Entr'ouvert dispose de deux administrateurs systèmes et de techniciens, habilités à effectuer les opérations de maintenance. 235

Des comptes nominatifs seront utilisés pour toute opération de maintenance, garantissant ainsi l'imputabilité des actions réalisées sur les serveurs.

Seules les clés SSH des personnes habilitées à effectuer les opérations de maintenance sont déclarées comme autorisées sur les serveurs, empêchant de fait l'accès à une personne qui ne détient pas l'habilitation. 240

## 8.9 Accès distants au système d'information de nos

Il n'y aura pas nécessité d'ouvrir des accès à distance aux serveurs hébergeant Publik.

Un accès SSH nominatif et temporaire pour certains membres de l'équipe technique d'Entr'ouvert pourra être utile lors du développement de connecteurs. 245

## 8.10 Architecture de sécurité

### 8.10.1 Contrôle et filtrage des flux

Les usagers accèdent à la plateforme uniquement en HTTPS. Les connecteurs communiquent entre eux via HTTPS ; une connexion avec des annuaires LDAP est possible avec filtrage des adresses IP. 250

Les administrateurs accèdent aux machines via le protocole SSH, limité aux adresses IP d'Entr'ouvert. Le port SSH est restreint, il n'est accessible que pour les administrateurs et certaines IP identifiés.

Les autres ports réseau sont fermés.

### 8.10.2 Confidentialité et intégrité des flux\*

255

Tous les flux sont chiffrés par des protocoles fiables (SSL, SSH, Ip Sec) sauf les e-mails émis par la plateforme.

### 8.10.3 Environnements

Les environnements de recette (nommée aussi test ou préproduction) sont identiques en terme de configuration et de logiciels avec l'environnement de production (avec néanmoins moins de ressources). Ils sont complètement isolés des environnements de production.

260

Les serveurs ne comportent que les logiciels nécessaires pour rendre le service et assurer la sécurité de ceux qui sont installés. Les services non nécessaires sont désinstallés ou désactivés s'ils ne peuvent pas l'être.

265

Il est possible d'installer un certificat conforme RGS. La fourniture de celui-ci est à la charge de .

## 8.11 Localisation des données

L'infrastructure de l'hébergement mutualisée est composée de serveurs répartis sur les centres de données français d'OVH (Roubaix, Gravelines et Strasbourg) en accès et sauvegarde.

270

## 8.12 Continuité d'activité

Nos services sont redondants et répliqués en continu afin d'assurer une disponibilité permanente.

- Les centres de données OVH sont certifiés ISO 27001.
- Les services sont redondants et répliqués en continu. Chaque nœud d'un cluster Publik dispose d'une copie synchrone de la base de données (postgresql hot-standby) et d'une synchronisation en temps réel des données (réplication

275

- DRBD). En cas de dysfonctionnement d'une machine, la continuité du service et l'intégrité des données sont assurées par une procédure de bascule éprouvée. 280
- Notre hébergeur nous fourni aussi une protection globale contre les dénis de service distribué.
  - Les services sont supervisés : une supervision générale est assurée par des agents logiciels qui remontent les informations sur la plateforme de surveillance et alertent les administrateurs d'Entr'ouvert en temps réel. 285
  - Des audits de sécurité sont régulièrement réalisés par des opérateurs indépendants.
  - Des sauvegardes complètes sont réalisées sur une machine isolée hors site; le système de restauration est régulièrement vérifié.
  - Archivage continu des bases-de-données et récupération de données à la minute (Point-in-time recovery). 290
  - Disponibilité garantie : >99,5% (99,74% constatés en 2019, les temps d'interruption relevant presque exclusivement de mises à jour nocturnes planifiées les seconds et quatrièmes jeudi de chaque mois).
  - Plan de continuité d'activité (PCA) : perte de données maximale admissible (PDMA/RPO) de 24 heures ouvrées. 295
  - Plan de reprise d'activité (PRA) : perte de données maximale admissible (PDMA/RPO) de 48 heures ouvrées.

### 8.13 Développement et sécurité

Entr'ouvert effectue une revue de code systématique. Celle-ci s'appuie sur des outils d'analyse statique de code lancés automatiquement et sur une relecture par un·e pair·e développeur·se d'Entr'ouvert. L'intégralité du code qui compose l'application Publik est ainsi systématiquement relue avant validation. 300

Les tests automatisés sont été intégrés au processus ("Intégration continue") pour s'assurer que le code est sécurisé avant la livraison. Les tests incluent aussi des analyses de code statiques pour détecter les vulnérabilités potentielles. Le serveur d'intégration d'Entr'ouvert est visible à l'adresse <https://jenkins.entrouvert.org/> 305

Les audits de sécurité sont effectués régulièrement par les clients d'Entr'ouvert sur la solution Publik. Les restitutions d'audits de sécurité peuvent donner lieu à la création de tickets dans le but d'apporter, lorsque nécessaire, des correctifs logiciels face aux éventuels problèmes identifiés. 310

Des audits de sécurité sont également menés sur la solution à l'initiative d'Entr'ouvert.

Nos développeurs et nos chefs de projets techniques sont au fait des dernières normes de sécurité et assure une veille sur les sujets de :

- Des normes de développement sécurisées
- Des menaces avancées persistances
- Des normes et évolutions de celles-ci concernant le RGPD

315

## 8.14 Appréciation des risques

Les risques identifiés pour le service Publik sont :

- DDOS (perte de disponibilité)
- Défaçage du site (perte de réputation)
- Injection de faux utilisateurs et de fausses demandes (perte d'intégrité des données)
- Fuite de données utilisateurs (perte de confidentialité)

320

Nos mesures de sécurisation prennent en compte les risques ci-dessus.

325

## 9 Matrice de couverture des exigences de sécurité

Le terme RACI est l'acronyme de « Réalisateur , Approbateur, Consulté et Informé

Action	Entr'ouvert	Hébergeur
Authentification et gestion des droits	C	R/A
Imputabilité, traçabilité	C	R/A -
Mises à jour, correctifs de sécurité	R/A	I -
Gestion des incidents de sécurité	R/A	I -
Protection contre les logiciels malveillants	R/A	I C
Sauvegardes et restaurations	R/A	- -
Supports de données et équipements sensibles	R/A	- R
Intervention des sociétés de maintenance ou de support	R/A	I R
Accès distants au système d'information de	I	R/A -
Architecture de sécurité	R/A	I C
Localisation des données	R/A	I C
Continuité d'activité	R/A	I R
Développement et sécurité	R/A	I -
Appréciations des Risques	R/A	I C

---

Action	Entr'ouvert	Hébergeur
--------	-------------	-----------

---

## 10 Documentation de suivi

Suivi des documents concernant la sécurité :

Nature du document	Date de remise	Commentaire
Plan d'Assurance Sécurité		
Comptes-rendus de réunion du comité de suivi	Une semaine après chaque réunion	