Guide pratique

Plan MonacoSanté Sécurité

Août 2026

Présentation du dispositif

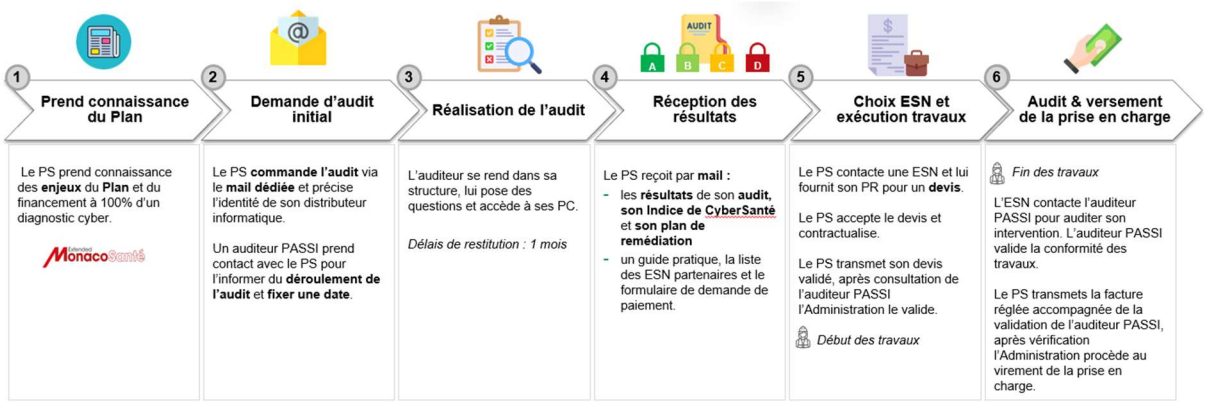
Le plan « MonacoSanté Sécurité » est porté conjointement par le Département des Affaires Sociales et de la Santé et la Délégation Interministérielle chargée de la Transition Numérique. Il a été conçu selon les recommandations de l'Agence Monégasque de Sécurité Numérique (AMSN). Il repose sur deux objectifs principaux :

- Auditer les systèmes d'information des acteurs de santé ;
- Prendre en charge une partie des frais de sécurisation des installations.

Il s'adresse aux acteurs de santé autorisés à exercer en Principauté de Monaco

1. Pourquoi bénéficier de MonacoSanté Sécurité ?
   - Un audit de sécurité pour découvrir les vulnérabilités cyber potentielles de votre système d'information, appréhender vos risques et définir votre stratégie de sécurisation, grâce aux recommandations d'experts.
   - La participation financière du Gouvernement pour sécuriser votre installation ;

2. Comment bénéficier du Plan MonacoSanté Sécurité ?



1. La demande d'audit initial

- Envoyer un e-mail à monacosantesecurite@gouv.mc avec vos coordonnées (nom, prénom, adresse et numéro de téléphone). Si vous travaillez déjà avec un prestataire informatique local, vous pouvez également le mentionner ;
- Un auditeur PASSI fixe un rendez-vous avec vous et réalise l'audit.

ℹ Vous vous engagez à être disponible sur le créneau réservé et à prévenir au moins 72h avant la structure d'audit et le gestionnaire du plan par e-mail, en cas d'annulation. Pour rappel, les audits sont financés entièrement par le Gouvernement Princier et ne nécessitent aucun paiement.

2. Réalisation de l'audit

- Le jour de l'audit, un auditeur vient dans vos locaux ;
- L'audit se divise en deux parties :

- Un questionnaire (environ 2h00 pour les professionnels libéraux) ;
- Une analyse de la sécurité de votre structure.

3. Réception des résultats de l'audit

- Vous recevez par e-mail les résultats de votre audit ainsi que le plan de remédiation. Ce dernier contient l'ensemble des mesures à prendre en compte pour corriger une/des failles ou une/des vulnérabilités cyber dans votre installation ;
- Vous obtenez également la liste des Entreprises de Services Numériques (ESN) partenaires du plan MonacoSanté Sécurité, habilitées à effectuer les travaux de sécurisation.

4. Recherche d'une ESN, devis et lancement du projet

- Contactez le prestataire technique de votre choix parmi la liste fournie et présentez-lui le plan de plan de remédiation pour guider la discussion ;
- Le prestataire fournit un devis chiffrant les travaux de remédiation nécessaires pour sécuriser votre structure, en reprenant en détail les préconisations contenues dans le plan de remédiation.

ℹ Pour rappel, le Gouvernement Princier finance à hauteur de 50% les prestations prévues dans la remédiation de votre structure, sur la base du devis validé. Seules les vulnérabilités cyber critiques et majeures contenues dans le plan de remédiation sont éligibles au financement, à l'exclusion des services annexes liés à l'hébergement. Le devis doit explicitement reprendre chaque vulnérabilité cyber critique ou majeure et l'associer à une action de remédiation.

- Le professionnel de santé décide du lancement du projet de sécurisation et signe le contrat avec le prestataire retenu. Il fait parvenir par mail le devis signé. L'auditeur PASSI valide que le devis reprend en détail les préconisations contenues dans le plan de remédiation. L'administration vous confirme par e-mail la prise en charge à hauteur de 50% des vulnérabilités cyber critiques et majeures. Le règlement est effectué en une seule fois à réception de la facture acquittée.

ℹ En cas de non-lancement des travaux, le professionnel de santé doit prévenir la structure d'audit de la non-poursuite du parcours de sécurisation.

5. Demande d'audit et versement de la prise en charge

Une fois les travaux de remédiation terminés, le prestataire contacte l'auditeur PASSI ayant réalisé l'audit afin de vérifier l'exécution des travaux.

L'auditeur PASSI convient d'un rendez-vous pour fixer l'audit de contrôle.

Une fois l'audit de contrôle effectué, l'auditeur envoie sa restitution par e-mail au professionnel de santé. Tant que l'audit de contrôle n'est pas conforme, le prestataire s'engage à y remédier sous 14 jours ouvrés,

Dès la conformité obtenue, le professionnel de santé transmet par e-mail à monacosantesecurite@gouv.mc la demande prise en charge contenant la restitution de l'audit de contrôle présentant un avis « conforme » ainsi que la facture réglée. Le Gouvernement Princier lui adresse en retour la participation financière.

Annexe :

Liste des prestataires informatiques

ESN	Mail de contact
SYSELIO	commercial@syselio.com
ACTIS	contact@actis.mc
SYCAMORE IT SARL	info@sycamoreit.com
ETHOS S.A.M.	info@ict-partners.mc
OPENSOLUTION	info@opensolution.mc
INFORMATION TECHNOLOGY IN MONACO (I.T.I.M.)	contact@itim.mc
GREEN IT CONSULTING S.A.R.L.	contact@greenit-monaco.com
HOMISIS	info@homisis.com
LUTESSA MONACO SARL	contact@lutessa.mc
MVE	info@mve.mc
I-QUASAR	info@i-quasar.com
SNS SOLUTIONS MONACO S.A.R.L.	monaco@snsolutions.fr
HELPERIANCE - BUGZERO	info@helperiance.com
ENGIT MONACO	info@engit.fr
INFOTEL MONACO SAM	rh.monaco@infotel.com
MONACO TECHNOLOGIES S.A.M.	info@monaco-technologies.com
WE+ MONACO S.A.M.	contact@we-plus.fr
S.A.R.L. ASTERIA	contact@asteria.mc
RBS MONACO	contact@rbs-entreprises.mc
SYNERGIE TECHNOLOGIES	contact@synergie.mc
ADEXCEL CONSULTING MONACO	contact-mc@adexcelconsulting.com
S.A.R.L. PARTNER CONSULTANCY MONACO	contactfrance@partnerconsultancyservices.com
MONACOM	info@monacom.mc