

RÉPUBLIQUE FRANÇAISE

Ministère de l'économie, des finances
et de la souveraineté industrielle,
énergétique et numérique

Décision du 22 septembre 2026 Portant homologation de sécurité de SIRHIUS – GAUdDI

NOR ECOP2620787S

L'autorité d'homologation,

Vu le référentiel général de sécurité pris en application du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives,

Vu la politique de sécurité des systèmes d'information de l'Etat publiée par circulaire du Premier ministre le 17 juillet 2014,

Vu la politique ministérielle de sécurité numérique des ministères économiques et financiers du 13 décembre 2023,

Vu la Décision du 21 octobre 2022 portant désignation de l'autorité d'homologation de sécurité de systèmes d'information du secrétariat général du ministère de l'Economie, des Finances et de la Souveraineté Industrielle et Numérique (NOR : ECOP2230648S),

Sur la base des échanges de la réunion de la commission d'homologation du 21 juillet 2026, réunissant les représentants du FSSI du MEFSIN, des RSSI (DGCCRF et SG), des MOAT et MOET du SIRH SIRHIUS et du SNUM, décide :

Article 1er

Le système d'information SIRHIUS et la brique GAUdDI sont homologués pour une durée de 3 ans à compter du 21 juillet 2026.

Article 2

Les risques résiduels à date sont acceptés et le **plan d'action** destiné à traiter ces risques est validé.

Ce plan d'action, présenté en annexe, comprend plusieurs actions dont celles de **priorité 1** sont détaillées ci-dessous.

Mettre en place l'authentification multi facteur (2FA) pour l'accès à la plateforme SIRHIUS.

- Dans un premier temps, mise du 2FA sur les SSO des directions des MEF et du MEAE.
- Puis dans un second temps, la généralisant ProConnect 2FA comme mécanisme de fédération des identités, en remplacement des comptes locaux et permettant une révocation homogène des accès.

Pseudonymiser l'environnement de recette de SIRHIUS

Assurer la prise en compte de la confidentialité des données RH par les prestataires et les utilisateurs et développer les moyens de contrôle.

- Etendre la charte de confidentialité à tous les utilisateurs de l'ensemble des directions ;
- Développer l'exploitation des traces de l'outil TRHACE
- Formaliser un plan d'assurance sécurité (PAS) avec les prestataires et une convention avec le CISIRH
- Vérifier les clauses de sécurité définies avec les prestataires

Implémenter la conservation des journaux techniques dans un puits centralisé, alimentant un service de détection

Compléter et finaliser le plan de continuité d'activité

Article 3

L'avancement du plan d'action sera évalué à 12 mois.

Article 4

Le chef du Service du Numérique est chargé de l'exécution de la présente décision, qui sera publiée au Bulletin officiel de l'administration centrale des ministères économiques et financiers.

Fait à Paris, le 22 septembre 2026

L'Autorité d'homologation

Jean Séverin LAIR

Chef du Service du Numérique du Secrétariat Général du MEFSIN

Annexes

Plan d'actions à mettre en œuvre issu de l'analyse de risque Répartition des actions par priorité

P1 : Priorité forte	P2 : Priorité modérée	P3 : Priorité faible
SOC-2 Vérifier les clauses de sécurité définies avec les prestataires du projet SIRHIUS et s'assurer de leur cohérence avec la politique des MEF (SOPRA, MC2I). SOC-7 Assurer la conservation des journaux technique sur une durée comprise entre 6 mois et 1 an, au sein d'un puits sécurisé et centralisé. SOC-8 Implémenter l'analyse de journaux techniques par un lien SOC ou dans un puit de log distinct non-accessible par les administrateurs technique SIRHIUS. SOC-10 Etablir des règles métier pour l'analyse des journaux fonctionnels (heures non ouvrées, localisation, actions inhabituelles, modifications suspectes etc.). MS-1/ MS-2 Formaliser un PAS avec les prestataires, en y intégrant un chapitre prévoyant la réalisation de contrôles visant à vérifier la conformité des engagements pris au titre de ce PAS. MS-3 Étendre la charte de confidentialité à tous les utilisateurs de l'ensemble des directions, afin qu'elle constitue un rappel clair des obligations prévues par la loi et par le droit de la fonction publique. Elle précisera les risques et sanctions associés à tout mésusage des données mises à disposition via SIRHIUS. MR-1 S'assurer de l'implémentation d'une méthode de pseudonymisation au sein de l'environnement de recette des colonnes de données sensibles. Conserver la table de correspondance des données pseudonymisées dans un environnement distinct et sécurisé. MR-4/SOC-5 Mettre en place l'authentification (2FA) pour l'accès à la plateforme SIRHIUS en généralisant ProConnect comme mécanisme de fédération des identités, en remplacement des comptes locaux et permettant une révocation homogène des accès.	SOC-4 Mettre en place le chiffrement au repos pour les données sensibles identifiées dans le cadre du DCPOD. SOC-9 Étudier la possibilité d'isoler la plateforme derrière un WAF. MR-2 Définir, au niveau applicatif, un quota maximal d'actions de consultation, téléchargement ou export autorisées par utilisateur sur une période donnée, déclenchant un blocage ou une alerte automatique en cas de dépassement. MR-5 Empêcher les administrateurs des habilitations de s'attribuer eux-mêmes des droits d'accès supplémentaires. MR-7 Mettre en place des alertes en cas de modification d'un volume anormalement élevé de données ou de documents du dossier dématérialisé. MR-8 Augmenter la précision et le détail des traces relatives aux consultations dans l'outil TRhace.	SOC-1 Appliquer le marquage sur la documentation technique (DAT, DEX, etc.). SOC-3 Préciser la localisation du stockage des sauvegardes et s'assurer de leur chiffrement. SOC-6 Définir les durées de rétention pour les traces des opérations d'administrations. MR-3 Renforcer la revue manuelle du code avant toute mise en production afin de détecter d'éventuels ajouts de code malveillants, et compléter ce contrôle par une analyse statique automatisée du code COBOL (SonarQube avec plugin COBOL) MR-6 Renforcer les contrôles de validation des référentiels et des flux entrants au niveau applicatif en automatisant et en affinant les vérifications déjà réalisées, en s'assurant que le format et le contenu des données reçues depuis les applications métiers des directions sont conformes aux spécifications attendues avant tout traitement.

Légende
■ Fait ■ En cours ■ A réaliser

Avancement sur le plan d'action :
0 action en place
4 actions en cours
17 actions non commencées

2 risques résiduels identifiés lors de l'analyse					
Risque	Description	Actions de réduction en cours de réalisation			Statut
R2	Un expert malveillant abuse de ses accès légitimes afin d'exfiltrer des données.	MS-3	Étendre la charte de confidentialité à tous les utilisateurs de l'ensemble des directions, afin qu'elle constitue un rappel clair des obligations prévues par la loi et par le droit de la fonction publique. Elle précisera les risques et sanctions associés à tout mésusage des données mises à disposition via SIRHIUS.	MISSION SIRHIUS & DSI Directions	A faire
		MR-2	Définir, au niveau applicatif, un quota maximal d'actions de consultation, téléchargement ou export autorisées par utilisateur sur une période donnée, déclenchant un blocage ou une alerte automatique en cas de dépassement.	MISSION SIRHIUS & DSI Directions	A faire
		MR-8	Augmenter la précision et le détail des traces relatives aux consultations dans l'outil TRhace.	SIRHIUS MOE	A faire
		SOC-10	Etablir des règles métier pour l'analyse des journaux fonctionnels (heures non ouvrées, localisation, actions inhabituelles, modifications suspectes etc.).	MISSION SIRHIUS & DSI Directions	A faire
R8	Compromission d'un expert (via une attaque par hameçonnage ou exploitation d'une vulnérabilité humaine) par un attaquant externe afin d'obtenir l'accès à aux données.	MS-3	Étendre la charte de confidentialité à tous les utilisateurs de l'ensemble des directions, afin qu'elle constitue un rappel clair des obligations prévues par la loi et par le droit de la fonction publique. Elle précisera les risques et sanctions associés à tout mésusage des données mises à disposition via SIRHIUS.	MISSION SIRHIUS & DSI Directions	A faire
		MR-2	Définir, au niveau applicatif, un quota maximal d'actions de consultation, téléchargement ou export autorisées par utilisateur sur une période donnée, déclenchant un blocage ou une alerte automatique en cas de dépassement.	MISSION SIRHIUS & DSI Directions	A faire
		MR-4	Mettre en place une double authentification (2FA) pour l'accès à la plateforme SIRHIUS en généralisant ProConnect comme mécanisme de fédération des identités, en remplacement des comptes locaux et permettant une révocation homogène des accès.	MISSION SIRHIUS & DSI Directions	En cours
		MR-8	Augmenter la précision et le détail des traces relatives aux consultations dans l'outil TRhace.	SIRHIUS MOE	A faire
		SOC-10	Etablir des règles métier pour l'analyse des journaux fonctionnels (heures non ouvrées, localisation, actions inhabituelles, modifications suspectes etc.).	MISSION SIRHIUS & DSI Directions	A faire