SYNDICAT MIXTE HAUTS DE FRANCE MOBILITES

COMITE SYNDICAL DU 8 juillet 2020

Délibération N° 2020 - 15

Objet : Commande d'une prestation d'accompagnement pour établir la certification RGS (Règlement Général de Sécurité)

Le Comité Syndical du Syndicat Mixte Hauts-de-France Mobilités réuni sous la présidence de son Président, Franck Dhersin, le 08 juillet 2020,

Vu le Code Général des collectivités territoriales,

Vu les statuts du Syndicat Mixte Hauts-de-France Mobilités,

Vu le Budget Primitif voté le 27 janvier 2020,

Vu l'ensemble des décisions budgétaires de l'exercice 2020 adoptées jusqu'à ce jour,

Vu l'instruction budgétaire et comptable de la M14,

Vu la délibération n° 2019 - 17 du 26 Juin 2019 relative au RGPD (Règlement Général de protection de la données) et la nécessité légale de recourir à un DPO,

Vu Le RGS (Règlement Général de Sécurité) élaboré conformément à l'article 9 de l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives ainsi qu'entre les autorités administratives.

CONSIDERANT

- Le caractère obligatoire de la certification RGS pour le système informatique PassPass.fr sous la responsabilité de Hauts de France Mobilités, tel qu'il en ressort de l'analyse du site effectuée par le DPO de Hauts-de-France Mobilité

DECIDE

- De commander à la société ADVENS, spécialisée dans le domaine des audits, conseils et réglementation en sécurité informatique, une prestation d'accompagnement pour accompagner Hauts-de-France Mobilités à l'obtention du certificat RGS du système centrale PassPass.fr, pour un montant de **25 770€**. Ce montant inclue un test d'intrusion du système qui permettra un rapport d'expertise d'ADVENS sur le niveau de sécurité actuel du système.

AUTORISE

Monsieur le Président à prendre les engagements juridiques, financiers et comptables nécessaires à l'exécution de la présente délibération.

Le Président,

Franck DHERSIN

Correspondance administrative : HDFM - Siège de Région - 151 Avenue du Président HOOVER 59555 LILLE CEDEX
Email : b.courty@hdfmobilites.fr - téléphone : 03 20 14 62 00

FICHE INFORMATIVE

Qu'est-ce que l'homologation RGS ?

La démarche d'homologation, recommandée (*) de longue date par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), est un préalable indispensable à l'instauration de la confiance dans les systèmes d'information et dans leur exploitation au quotidien. Il s'agit d'un processus d'information et de responsabilisation qui aboutit à une décision, prise par le responsable de l'organisation. Cette décision constitue un acte formel par lequel :

- Il atteste de sa connaissance du système d'information et des mesures de sécurité (techniques, organisationnelles ou juridiques) mises en œuvre.
- Il accepte les risques qui demeurent, aussi appelés risques résiduels.

Pour être efficace, la démarche d'homologation doit être adaptée aux enjeux de sécurité du système, notamment au contexte d'emploi, à la nature des données contenues, ou encore aux utilisateurs...

(*) *La réglementation rend obligatoire l'homologation pour les systèmes d'information traitant d'informations classifiées de défense (IGI 1300) et ceux permettant des échanges entre une autorité administrative et les usagers, ou entre autorités administratives (RGS).*

Contenu / démarche de la prestation d'accompagnement de la société ADVENS

1. Réaliser l'analyse de risque

- Réaliser des ateliers avec les parties prenantes pour identifier
  - Les actifs (essentiels et supports)
  - Leurs besoins de sécurité (DIC[T])
  - Les événements redoutés et leurs conséquences en termes d'image, d'activité, financier et légale
  - Les menaces, vulnérabilités et leurs vraisemblances en prenant en compte les incidents survenus et, si cette option est choisie, les résultats du test d'intrusion
- Définir les scénarios de risques
- Constituer les risques et leurs niveaux
- Définir le plan de traitement des risques
- Identifier les mesures organisationnelles et techniques
- Etablir les risques résiduels
- Restituer
- Présenter les risques aux différentes parties prenantes pour acceptation

2. Accompagner à la constitution du dossier d'homologation RGS

Hormis l'analyse de risque, HDFM formalisera le dossier d'homologation, dont :

- La stratégie d'homologation
- L'analyse de risque
- Le support pour la commission d'homologation

→ Advens peut fournir les modèles des documents ci-dessus

→ Advens accompagnera HDFM lors de la constitution du dossier et validera ce dernier

3. Réaliser un test d'intrusion informatique

Le test d'intrusion suit une démarche similaire à celle employée par une personne souhaitant commettre un acte de malveillance permettant meilleure identification des risques.

- Possibilités d'atteinte à votre image de marque,
- Vol d'informations confidentielles, financières et à caractère personnel,
- Attaques sur le navigateur des utilisateurs légitimes,
- Usurpation d'identité,
- Contournement des restrictions d'accès et élévation de privilèges,

Livrable : Rapport d'audit détaillé sur le niveau global de sécurité du système et les axes d'amélioration possibles