

Service départemental d'incendie et de secours de la Charente-Maritime

Bureau du Conseil d'administration

Séance du 10 juin 2024

Extrait des délibérations

Le 10 juin 2024, le Bureau du Conseil d'administration du SDIS 17 s'est réuni au centre de commandement du SDIS à Périgny, sur convocation du président, Monsieur Stéphane VILLAIN et sous sa présidence.

Date de la convocation : le 3 juin 2024.

Etaient présents Madame, Monsieur : Bernard BESSON, Jean-Claude GRENON, Ghislaine GUILLEN

Etait excusé Monsieur : Christophe CABRI.

Nombre de conseillers en	exercice :	5
	quorum :	3
	présents :	4

N°54-2024

HOMOLOGATION RGS

Le Bureau du Conseil d'administration du service départemental d'incendie et de secours de la Charente-Maritime,

Vu le Code général des collectivités territoriales,

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

Vu le référentiel général de sécurité version 2.0 approuvé par l'arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques ;

Vu la délibération n°35-2023 du Conseil d'administration du 14 mars 2023 ;

Vu le rapport du président du Conseil d'administration,

HOMOLOGATION RGS

L'actualité rappelle régulièrement que les SDIS sont une cible de choix pour les cyber-criminels. Depuis quelques mois, la Dordogne, le Lot-et-Garonne, les Pyrénées-Atlantiques et le Loiret ont subi des attaques qui, sans mettre les établissements dans l'incapacité d'accomplir leurs missions de secours, ont néanmoins provoqué une profonde désorganisation de leurs services.

Le CASDIS du 14 mars 2023 a adapté l'organisation du groupement des systèmes d'information dans l'objectif de renforcer la sécurité du Système d'information (SI). Aujourd'hui les équipes techniques surveillent au quotidien le fonctionnement des dispositifs de protection (pare-feu, anti-virus), procèdent aux mises à jour de sécurité et corrigent, chaque fois que c'est possible, les failles identifiées (mots de passe « faibles », phishing, comptes inactifs,...) dans un contexte d'évolution très rapide de la menace.

En parallèle de ces actions permanentes, une démarche plus en profondeur a été conduite avec l'appui de SOLURIS. Elle a permis d'analyser le niveau de sécurité actuel du SI et de définir un niveau de sécurité cible à atteindre sur le long terme. Il s'agit d'inscrire l'établissement dans un processus d'amélioration continue, à la fois pragmatique et adapté, en tenant compte de ses capacités humaines et financières. Cette démarche se traduit par la proposition d'homologation au Référentiel Général de Sécurité (RGS).

Ce dispositif, créé par l'ordonnance n°2005-516 du 8 décembre 2005, vise à renforcer la confiance des usagers dans les services électroniques, notamment lorsque ceux-ci traitent des données personnelles, mais aussi à organiser les échanges numériques entre autorités administratives. Il sera bientôt renforcé par la transposition en droit français de la directive européenne NIS 2 qui étend le périmètre d'application des mesures de sécurité cyber aux établissements qui, comme les SDIS, sont jugés essentiels au fonctionnement des états membres et durcit les sanctions en cas de manquements.

Les travaux qui se sont déroulés entre janvier et mai 2024 ont comporté plusieurs grandes étapes :

- une analyse des risques et des vulnérabilités s'appuyant sur 114 points de contrôle ;
- la définition des objectifs de sécurité ;
- le choix et la proposition de mise en œuvre des mesures appropriées de protection et de défense du Système d'Information et de Communication (SIC) ;
- la préparation du dossier d'homologation de sécurité du système d'information.

Ils se sont appuyés sur plusieurs référentiels dont le guide de l'ANSSI intitulé « L'homologation de sécurité en 9 étapes simples » qui décrit de manière plus détaillée la démarche à réaliser pour produire un dossier d'homologation en appui à la décision d'homologation prononcée par l'autorité administrative.

Accompagné par le syndicat mixte SOLURIS, le SDIS 17 a réalisé les activités exigées pour prononcer l'homologation de sécurité au RGS de son Système d'Information et de Communication. L'ensemble des résultats a été consolidé dans le présent document.

Le SDIS 17 possède désormais un Système de Management de la Sécurité de l'Information (SMSI) et une Politique de Sécurité de son Système d'Information et de Communication (PSSIC) documentée, appliquée, révisée et contrôlable.

Après en avoir délibéré, le Bureau du Conseil d'administration décide, à l'unanimité :

- d'approuver l'homologation de sécurité du Système d'Information et de Communication du SDIS et d'autoriser le Président du Conseil d'administration à signer tous les actes en découlant.

Fait et délibéré les jour, mois et an susdits.

Le Président du Conseil d'administration

Stéphane VILLAIN



Certifié, publié et exécutoire

le 11 JUIN 2024

B10062024 DEL 54

Pour le Président du conseil d'administration
et par délégation
le Directeur départemental

Contrôleur général Didier Marcaillou